

Maintaining, Updating, and Protecting Windows 7

LESSON

7

EXAM OBJECTIVE MATRIX

SKILLS/CONCEPTS	EXAM OBJECTIVE DESCRIPTION	EXAM OBJECTIVE NUMBER
Exploring Built-in Maintenance Tools	Understand maintenance tools.	6.2
Maintaining the Windows Registry	Remove malicious software.	3.3
Updating the System	Understand updates.	6.3
Defending Your System from Malicious Software	Remove malicious software.	3.3

KEY TERMS

Action Center

Disk Cleanup

Disk Defragmenter

endpoint

firewall

fragmented

hotfix

malicious software (malware)

Microsoft Forefront Endpoint Protection

Microsoft Security Essentials

Microsoft Update

Microsoft Windows Malicious Software
Removal Tool

service pack

signature

spyware

Task Scheduler

trigger

Windows Defender

Windows Firewall

Windows registry

Windows Update

A primary part of your IT technician position at Interstate Snacks involves maintaining company computers. To keep support costs down, you use free tools that are built into Windows or downloadable from the Microsoft Web site. The tools include Disk Defragmenter, Disk Cleanup, Windows Update, Windows Defender, and Microsoft Security Essentials. With the exception of Disk Cleanup, these tools have built-in scheduling features. You plan to use Task Scheduler to automate Disk Cleanup to run once a week and to start the accounting software every day at 8:30 a.m. for all accounting employees.

■ Exploring Built-in Maintenance Tools



Windows 7 comes with many built-in maintenance tools that help to keep computers running at top performance. These tools include Disk Defragmenter, Disk Cleanup, Task Scheduler, and the Action Center Maintenance feature.

Microsoft began bundling computer maintenance utilities in its early versions of Windows and has improved and expanded on them ever since. The latest utilities provide nearly any type of maintenance you might need, such as defragmenting disks, removing unnecessary files, scheduling tasks, troubleshooting problems, backing up files, and more.

In the following sections, you learn about some of the most popular Windows built-in utilities: Disk Defragmenter, Disk Cleanup, Task Scheduler, and the Maintenance section of Action Center. You can find many of the maintenance tools in the System Tools folder (click **Start > All Programs > Accessories > System Tools**).

Understanding Disk Defragmenter

Disk Defragmenter can speed up your computer's performance by defragmenting data on your hard disk. In Windows 7, the utility is set to automatically run once a week.

CERTIFICATION READY

What is Disk Defragmenter?

6.2

A hard disk is divided into many sectors, each of which can hold a small amount of data for a file. The hard disk's arm moves across a disk to "read" each sector in order to display a file or run a program. As more and more files are added to the disk the information becomes *fragmented*, which means it is spread across sectors on different parts of the disk.

Disk Defragmenter is a utility that helps improve your computer's performance by moving sectors of data on the hard disk, so that files are stored sequentially. This minimizes the movement a hard disk's arm must make to read all of the sectors that make up a file or program.

TAKE NOTE *

Solid state drives (SSDs) differ from hard disks. An SSD uses solid state memory to store data rather than writing data to sectors. Therefore, an SSD does not need to be defragmented.

Disk Defragmenter first analyzes your hard disk to determine the level of fragmentation, and then it defragments the disk if necessary.

In Windows 7, Disk Defragmenter is scheduled to run once a week by default. Although you may continue to use your computer while your hard disk is being defragmented, you might notice a performance hit if you're working on large files or running several programs at once, for example. If you're often working on your computer when the hard disk is being analyzed and defragmented, you can change the schedule when Disk Defragmenter runs automatically.



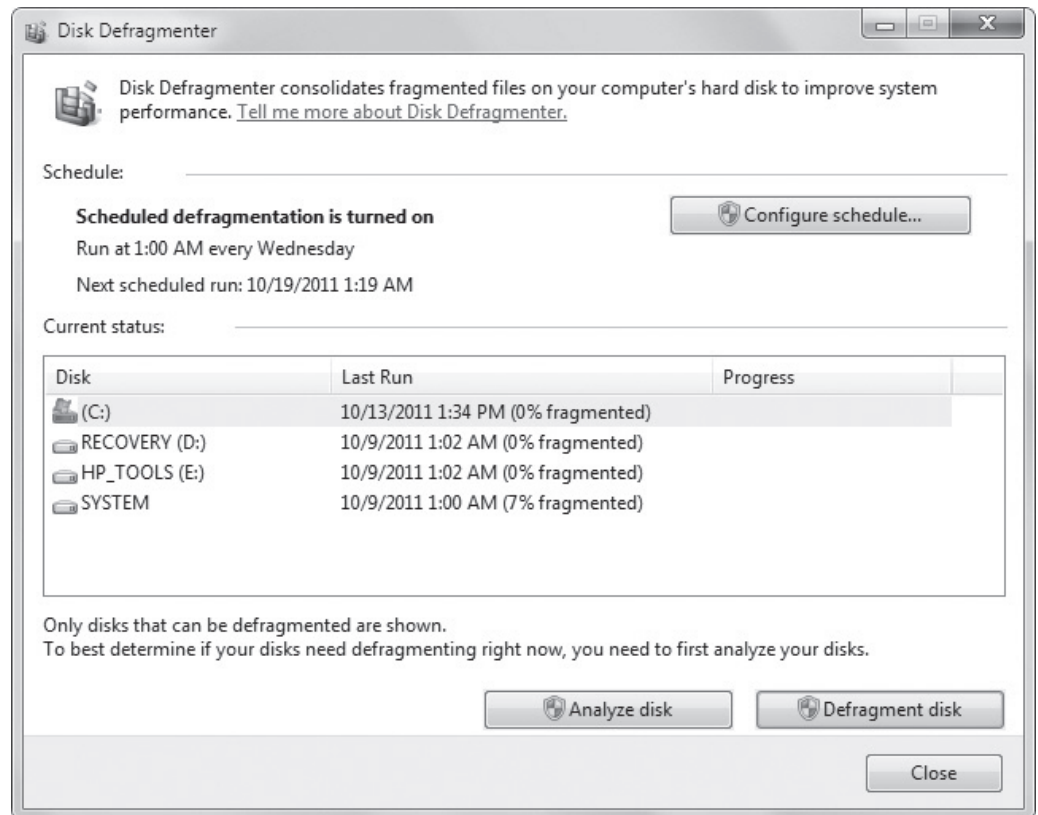
RUN DISK DEFRAGMENTER

GET READY. To run Disk Defragmenter, perform the following steps:

1. Click **Start > All Programs > Accessories > System Tools > Disk Defragmenter**. (Alternately, click **Start** and in the **Search programs and files** search box, type **defrag** and then click **Disk Defragmenter** from the resulting list.) If prompted for administrative privileges, type the password or provide confirmation.

Figure 7-1

The Disk Defragmenter window



2. Click **Defragment disk**.

The defragmentation process can take several minutes to well over an hour to complete, depending on the size and level of fragmentation of the hard disk.

IT technicians and other advanced users may want to use the command-line version of Disk Defragmenter, in order to run reports and use advanced commands. To use the utility at a command-line, click **Start**, type **cmd** in the *Search programs and files* search box, select **cmd.exe** from the resulting list, and then in the command window, type **defrag/?** and press **Enter**. Re-issue the command using any of the command-line parameters that display.



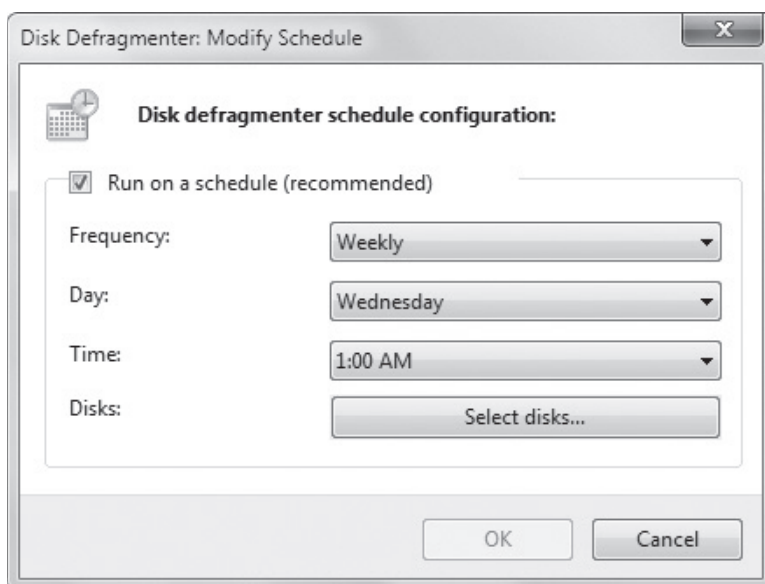
CHANGE THE DISK DEFRAGMENTER SCHEDULE

GET READY. To change the Disk Defragmenter schedule, perform the following steps:

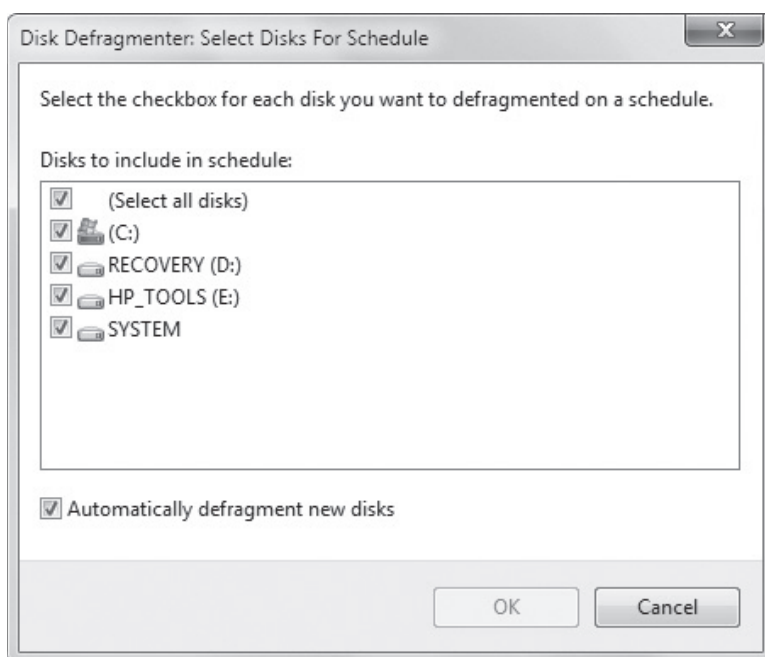
1. In Disk Defragmenter (refer to Figure 7-1 if necessary), click **Configure schedule**. The Disk Defragmenter: Modify Schedule dialog box displays (see Figure 7-2).
2. To change how often Disk Defragmenter runs, click the Frequency drop-down arrow and select **Daily**, **Weekly**, or **Monthly**. If you choose **Weekly** or **Monthly**, click the Day drop-down arrow, and select a day of the week or a day of the month.
3. To change the time of day when Disk Defragmenter runs, click the **Time** drop-down arrow and select a time.
4. To change the volumes that are scheduled to be defragmented, click the **Select disks** button (see Figure 7-3). Deselect any volumes you don't want scanned, and then click **OK**.
5. Click **OK**, and then click **Close**.

Figure 7-2

Disk Defragmenter: Modify Schedule dialog box

**Figure 7-3**

Disk Defragmenter: Select Disks For Schedule dialog box



+ MORE INFORMATION

To learn more about improving disk performance with Disk Defragmenter, visit <http://windows.microsoft.com/en-US/windows7/Improve-performance-by-defragmenting-your-hard-disk>

Understanding Disk Cleanup

Disk Cleanup helps you remove unnecessary files from your computer, such as downloaded program files, temporary Internet files, those that are left after running software, and much more.

CERTIFICATION READY

How does Disk Cleanup help you maintain a Windows 7 computer?

6.2

Another handy maintenance tool in Windows 7, and many previous versions of Windows, is **Disk Cleanup**. This utility removes many different kinds of unnecessary files from your computer:

- Downloaded program files
- Temporary Internet files
- Offline Web pages
- Files in the Recycle Bin
- Setup log files
- Temporary files left by programs, often in a TEMP folder
- Thumbnails for photos, videos, and documents used by the Windows interface (if you delete them, Windows re-creates them when needed)
- Windows error reporting files

You choose which files are deleted by Disk Cleanup by selecting and deselecting the boxes for each.

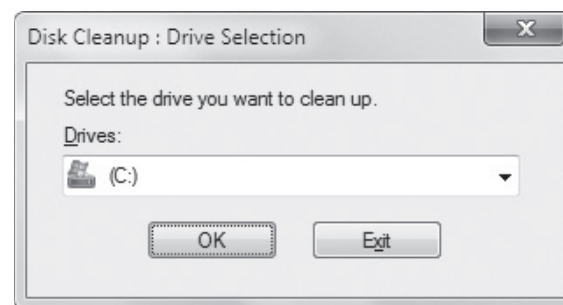
**RUN DISK CLEANUP**

GET READY. To run Disk Cleanup, perform the following steps:

1. Click **Start > All Programs > Accessories > System Tools > Disk Cleanup**. (Alternately, click **Start** and in the **Search programs and files** search box, type **clean** and then click **Disk Cleanup** from the resulting list.) If prompted for administrative privileges, type the password or provide confirmation.
2. The Disk Cleanup: Drive Selection dialog box displays (see Figure 7-4). In the **Drives** drop-down list, click the arrow to select the drive you want to clean and then click **OK**.

Figure 7-4

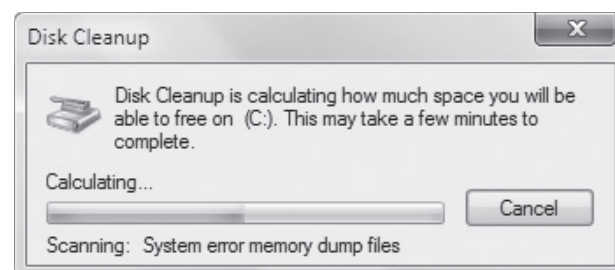
Selecting a drive for Disk Cleanup to scan



Disk Cleanup scans your disk (see Figure 7-5) to determine how much space it can free up. (You can safely click **Cancel**, if necessary, but you will have to restart Disk Cleanup to clean your disk.)

Figure 7-5

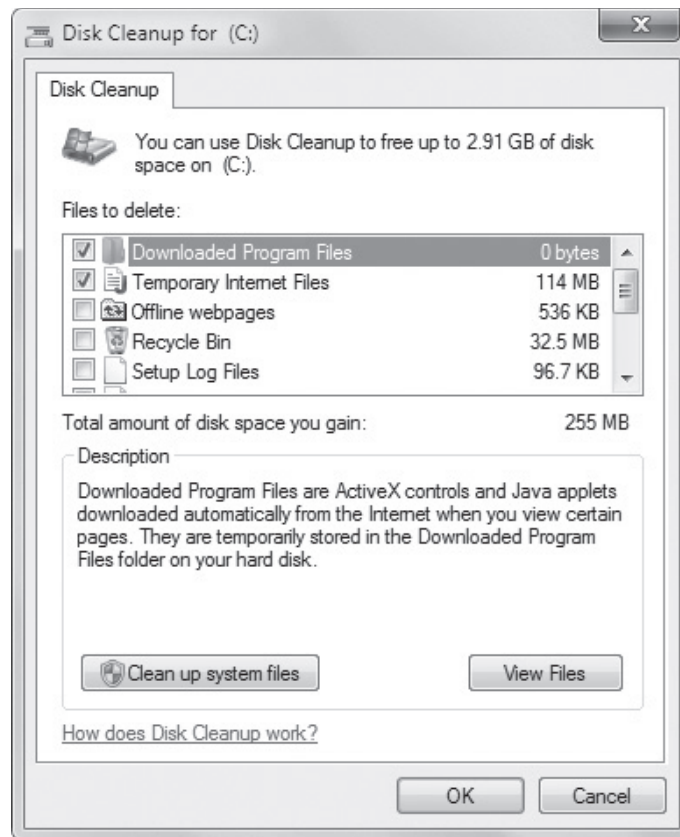
Disk Cleanup scanning a disk



3. The Disk Cleanup dialog box for the selected drive displays (see Figure 7-6). Select the types of files you want the utility to delete; those that are deselected will not be deleted. For many of the file types, you can click **View Files** to see a list of files that will be deleted.

Figure 7-6

The Disk Cleanup dialog box



4. When you're ready, click **Clean up system files**.

+ MORE INFORMATION

To learn more about using Disk Cleanup and the types of files it deletes, visit <http://windows.microsoft.com/en-US/windows-vista/Delete-files-using-Disk-Cleanup>

Understanding Task Scheduler

Many, but not all, Windows utilities have their own scheduling feature. For those utilities that you want to automate, you can use Task Scheduler. You can also use Task Scheduler to open programs on specific days and times, or at Windows startup.

CERTIFICATION READY

How do you use Task Scheduler to automate tasks?

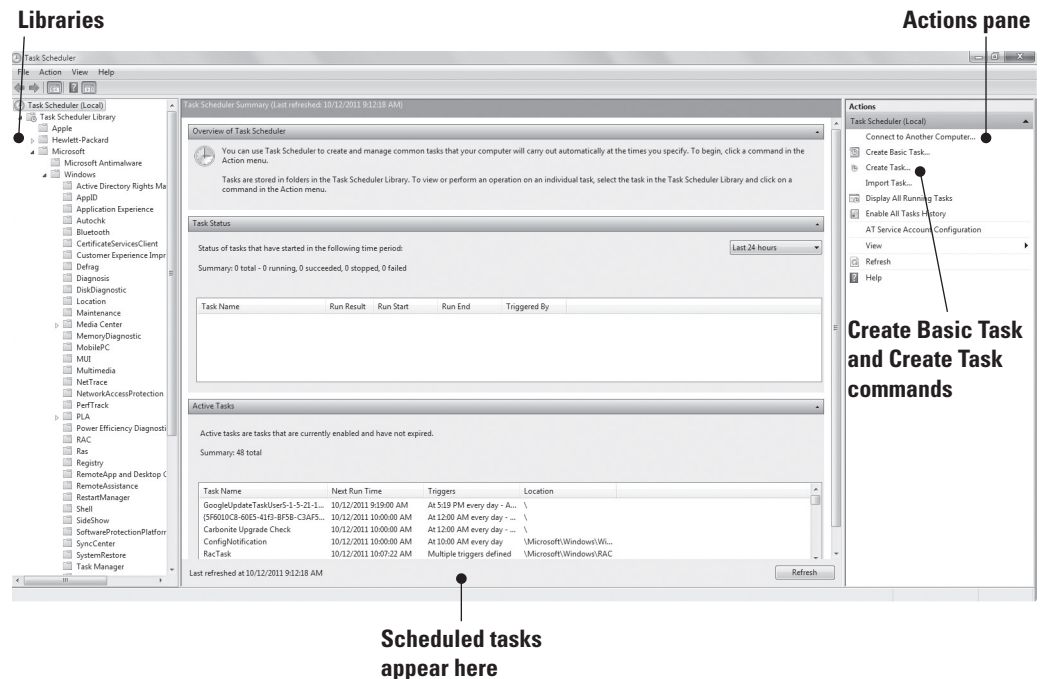
6.2

Task Scheduler enables you to schedule and automate a variety of actions, such as starting programs, displaying messages, and even sending e-mails. You create a scheduled task by specifying a **trigger**, which is an event that causes a task to run, and an **action**, which is the action taken when the task runs.

The main Task Scheduler window is shown in Figure 7-7. The left pane lists the Task Scheduler Library, which contains several built-in tasks by Microsoft and other vendors.

Figure 7-7

The main Task Scheduler window with the built-in task libraries expanded



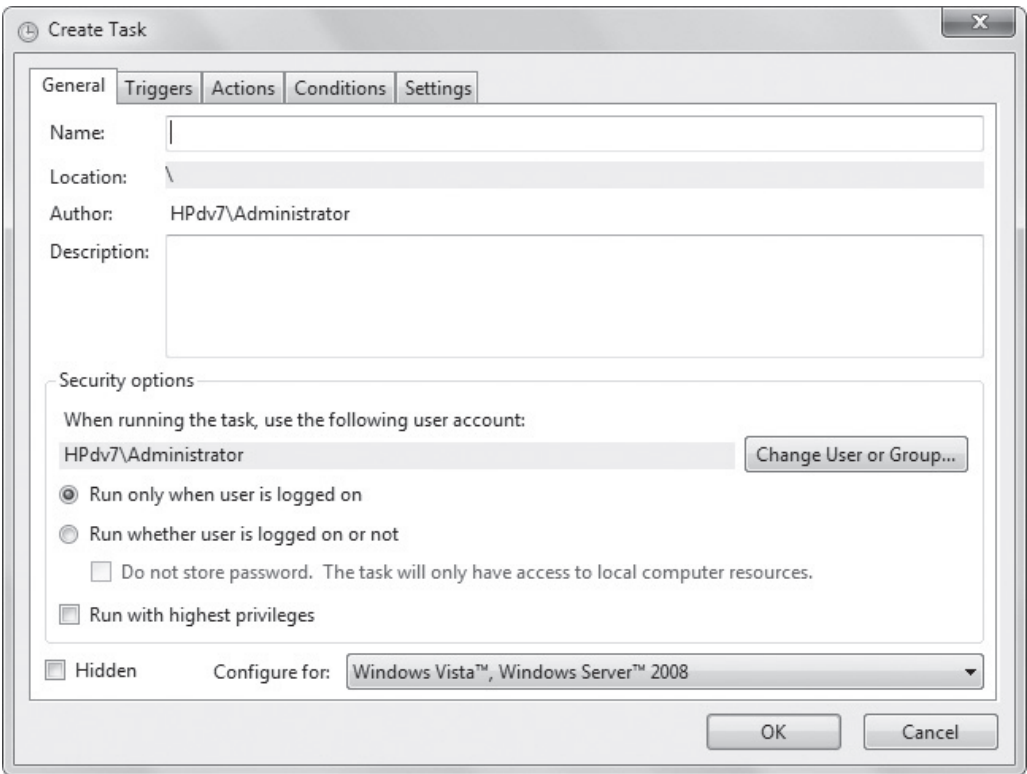
The middle pane has three panes. The Overview pane gives you an overview of Task Scheduler, the Task Status pane displays a summary of tasks that started in a certain time period (for example, within the last 24 hours), and the Active Tasks pane displays scheduled tasks. The information displayed in the middle pane can vary greatly from computer to computer.

On the right of the screen, the Actions pane provides commands for connecting to another computer and scheduling tasks for that computer, creating basic and more advanced tasks, and commands for viewing tasks and their histories. Notice in Figure 7-7 that there are two commands in the Actions pane for creating tasks: Create Basic Task and Create Task. When you use the Create Basic Task command, the Create Basic Task Wizard walks you through the essentials of creating a task. The Create Task command displays the Create Task dialog box (see Figure 7-8), which is the manual way of creating task but gives you more control and options.

To schedule tasks for all users on your computer, you must be logged on as the Administrator. If you're logged on as a Standard user, you can schedule tasks only for your user account.

Figure 7-8

The General tab



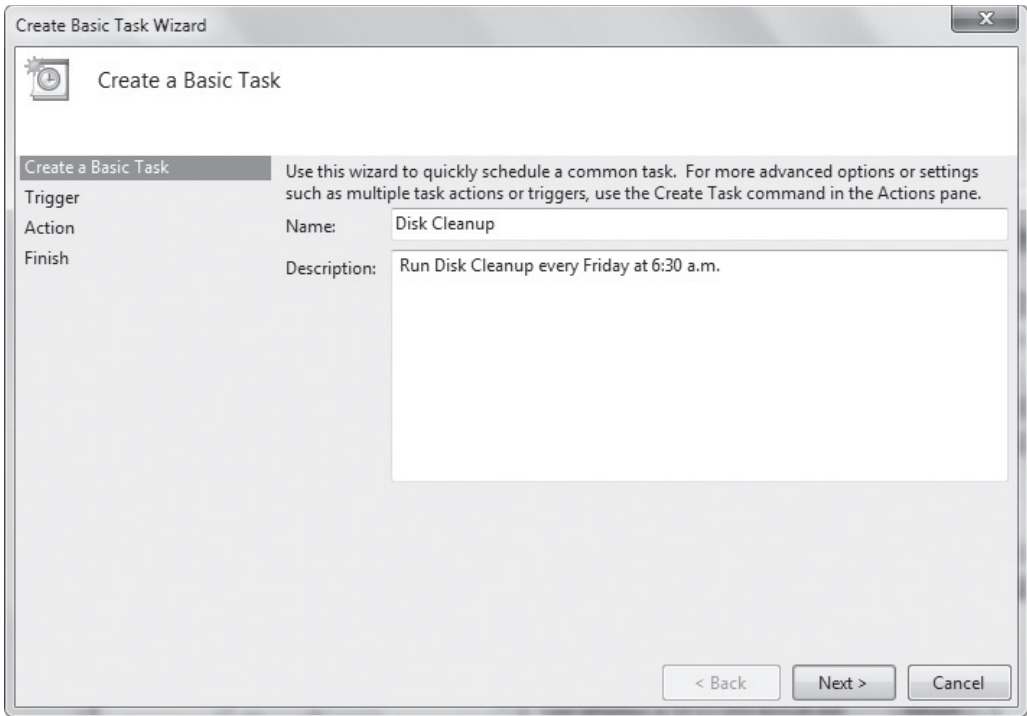
CREATE A TASK USING THE CREATE BASIC TASK WIZARD

GET READY. To create a task using the Create Basic Task Wizard, perform the following steps:

- 1. Click **Start > All Programs > Accessories > System Tools > Task Scheduler**.
(Alternately, click **Start** and in the **Search programs and files** search box, type **task**, and then click **Task Scheduler** from the resulting list.)

Figure 7-9

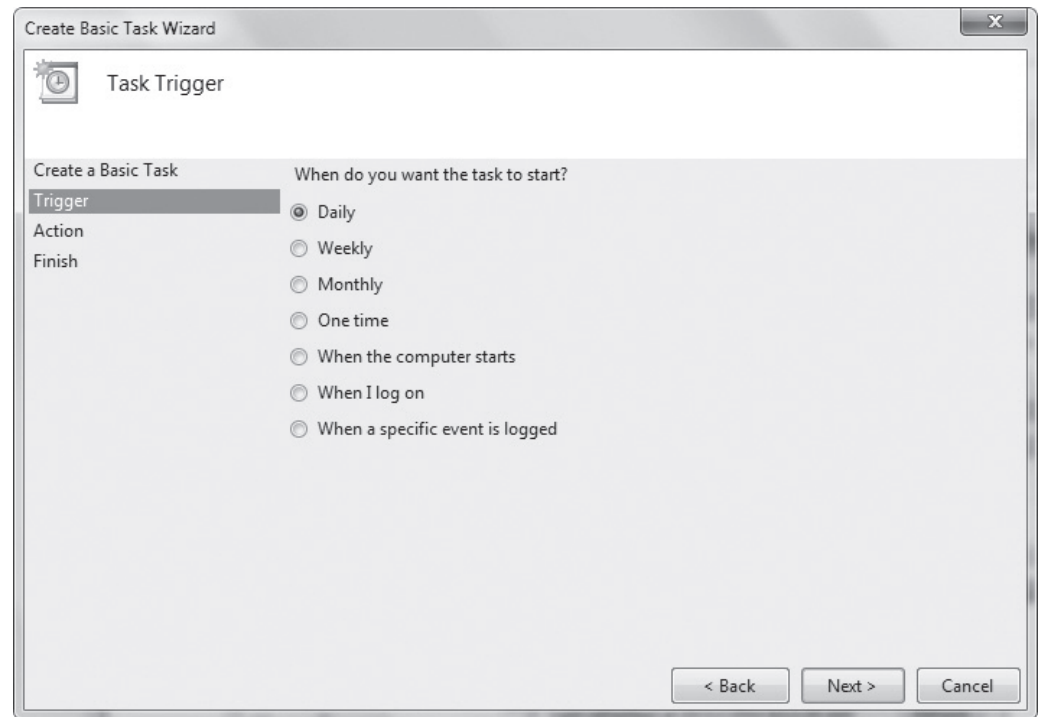
Entering information for a basic task in the initial wizard screen



2. In the Actions pane on the right, click **Create Basic Task**. The Create Basic Task Wizard starts.
3. In the initial screen, type a name for the task and its description (optional). In the example shown in Figure 7-9, the Task Scheduler will run Disk Cleanup every Friday at 6:30 a.m. Click **Next**.
4. The Task Trigger screen enables you to select the frequency the task should occur or an event that triggers the task (see Figure 7-10). The default selection is Daily. For our example, because this task will run weekly, click the **Weekly** radio button and then click **Next**.

Figure 7-10

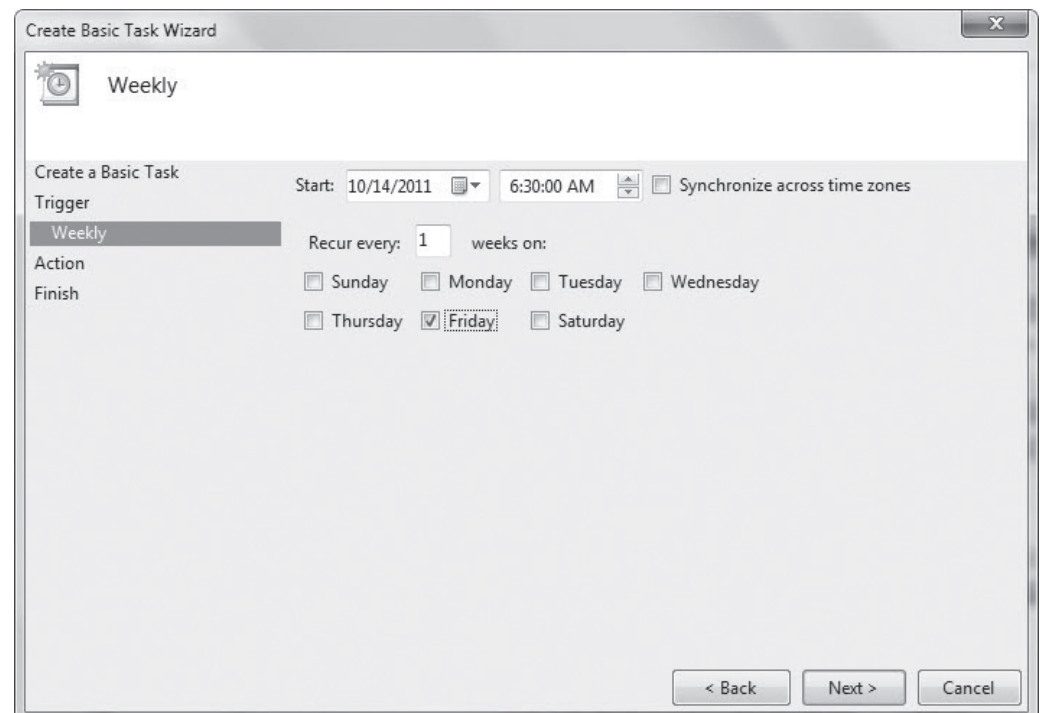
You can create a task to run daily, weekly, monthly, one time, and more



5. In the Weekly screen, select a starting date as well as the time and day of the week the task should run (see Figure 7-11). Click **Next**.

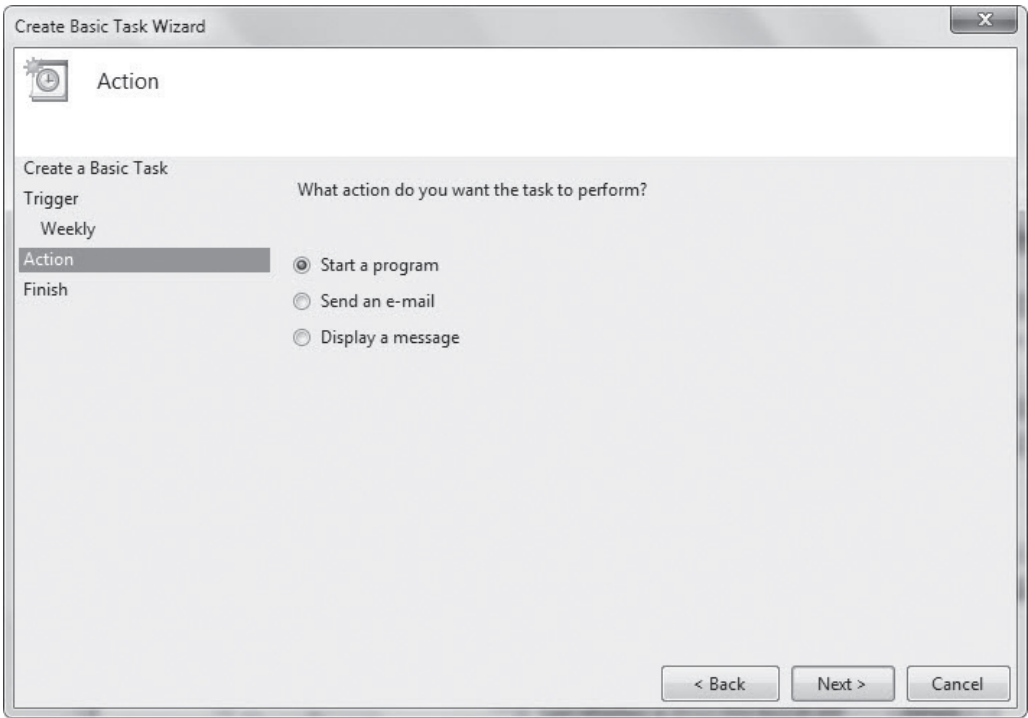
Figure 7-11

Selecting frequency and recurrence of the task



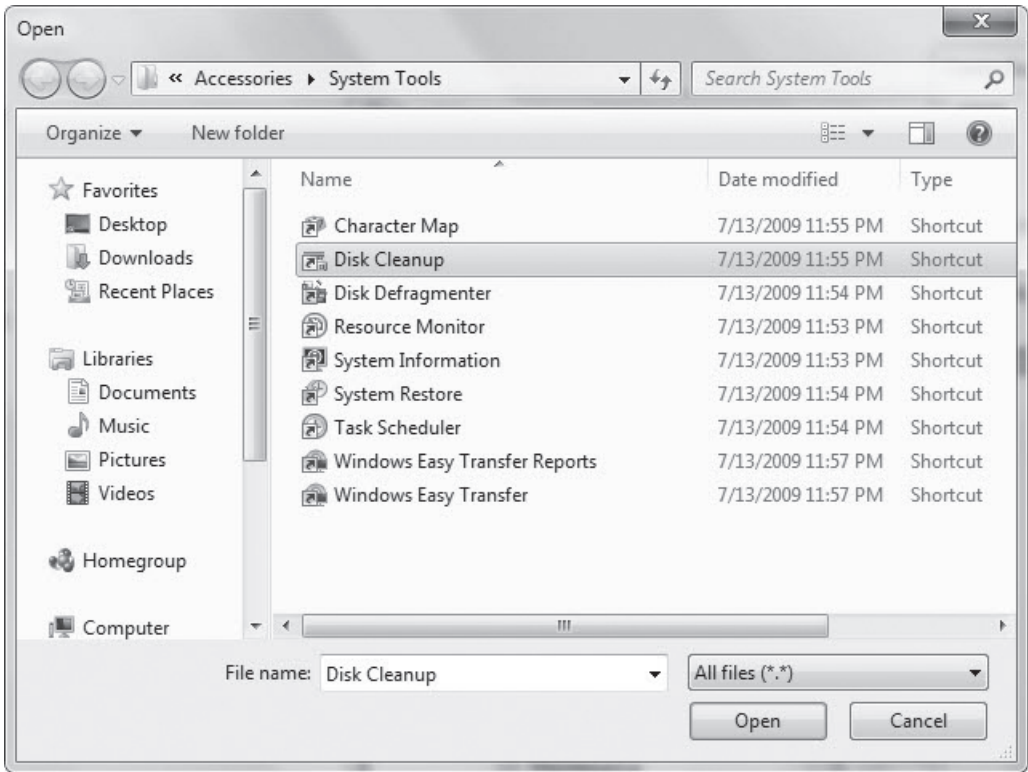
- 6. On the Action screen (see Figure 7-12), select the action that will be performed when the task runs. Because in this example we want to start a program, leave the default selected and then click **Next**.

Figure 7-12
Selecting the action to be performed



In the Start a Program window that displays, click **Browse** to find the Disk Cleanup program. The window shown in Figure 7-13 displays.

Figure 7-13
Selecting the program to run

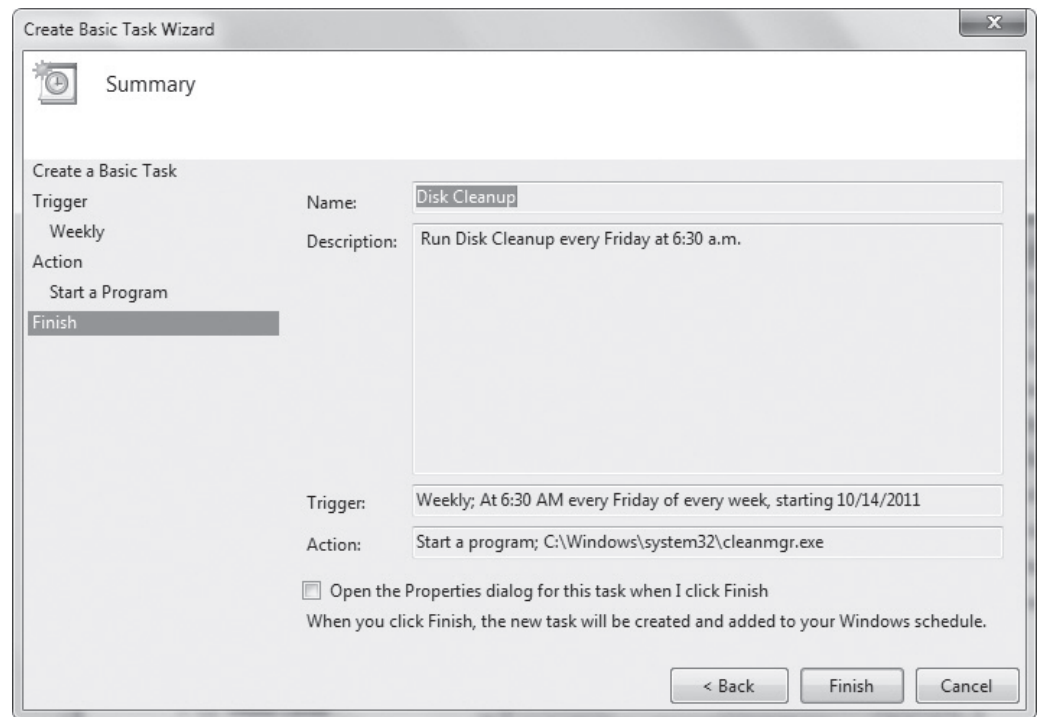


Click **Disk Cleanup** and then click **Open**. (If the window in Figure 7-13 does not display, navigate to the Disk Cleanup executable file in C:\Windows\system32\cleanmgr.exe, click **cleanmgr.exe**, and then click **Open**.) When the Start a Program screen displays again, which now indicates the path to the Disk Cleanup program executable, click **Next**.

7. The Summary screen summarizes the task, indicating when it will run (see Figure 7-14). If everything is correct, click **Finish**. If you need to make any changes, click the **Back** button, make the appropriate changes, and then click **Finish**.

Figure 7-14

Finishing the task creation



The task is added to Task Scheduler and will run on the trigger date.



CREATE A TASK MANUALLY

GET READY. To create a task manually, such as scheduling a program to start when Windows starts, perform the following steps:

1. In Task Scheduler, in the Actions pane, click **Create Task**.
2. In the Create Task dialog box, on the General tab, type a **Name** for the task and a **Description** (optional). In the Security Options section, you can click **Change User or Group** to change the account or group the task runs under, and select whether the task should run when the user is logged on or not. Be sure to select the appropriate operating system in the **Configure for** drop-down list. The completed tab is shown in Figure 7-15.
3. Click the **Triggers** tab, and then click **New**. In the New Trigger dialog box, click the **Begin the task** drop-down arrow (see Figure 7-16) and select one of the options, such as **At startup**.

Figure 7-15
Adding information to the General tab

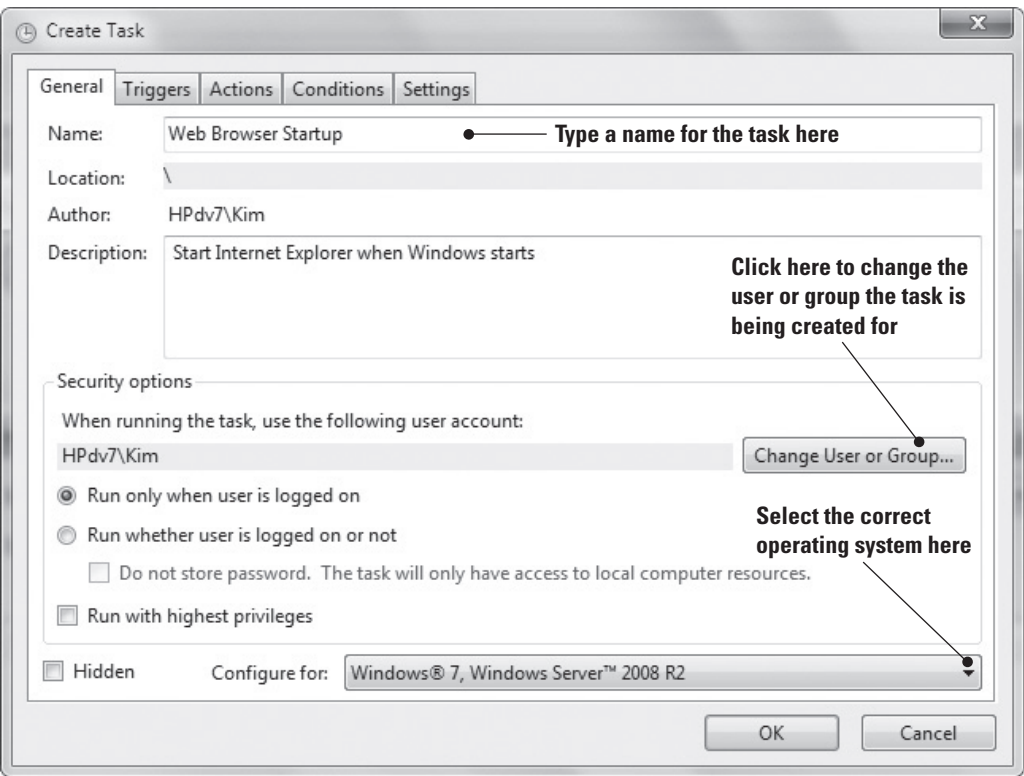
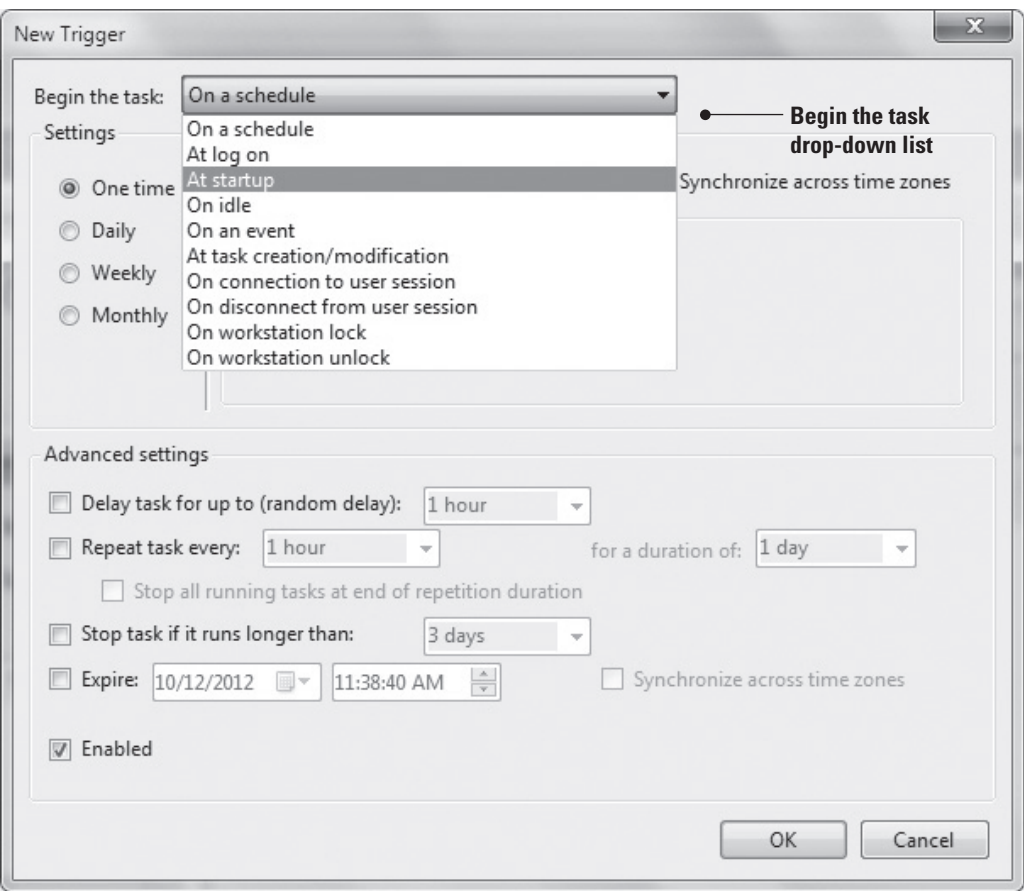


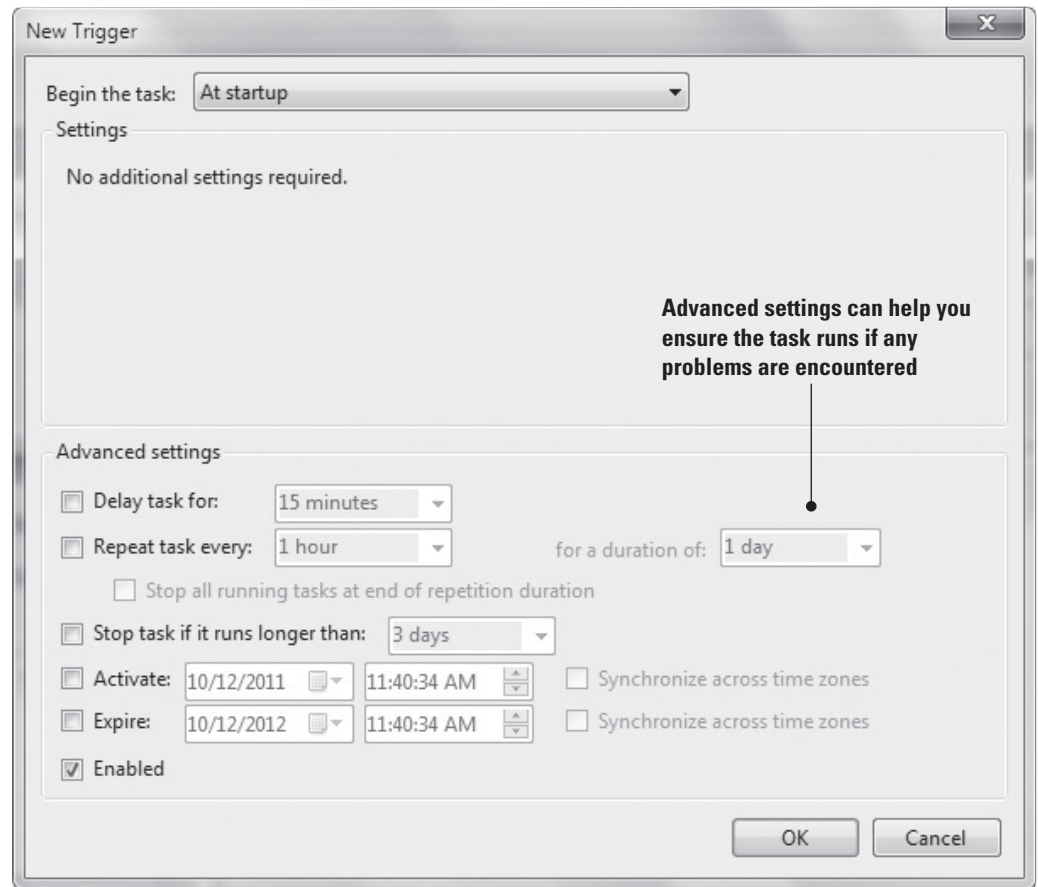
Figure 7-16
The New Trigger dialog box



With this option selected, the New Trigger dialog box changes (see Figure 7-17). Configure advanced settings, if needed, and then click **OK**.

Figure 7-17

The New Trigger dialog box after selecting the At startup option



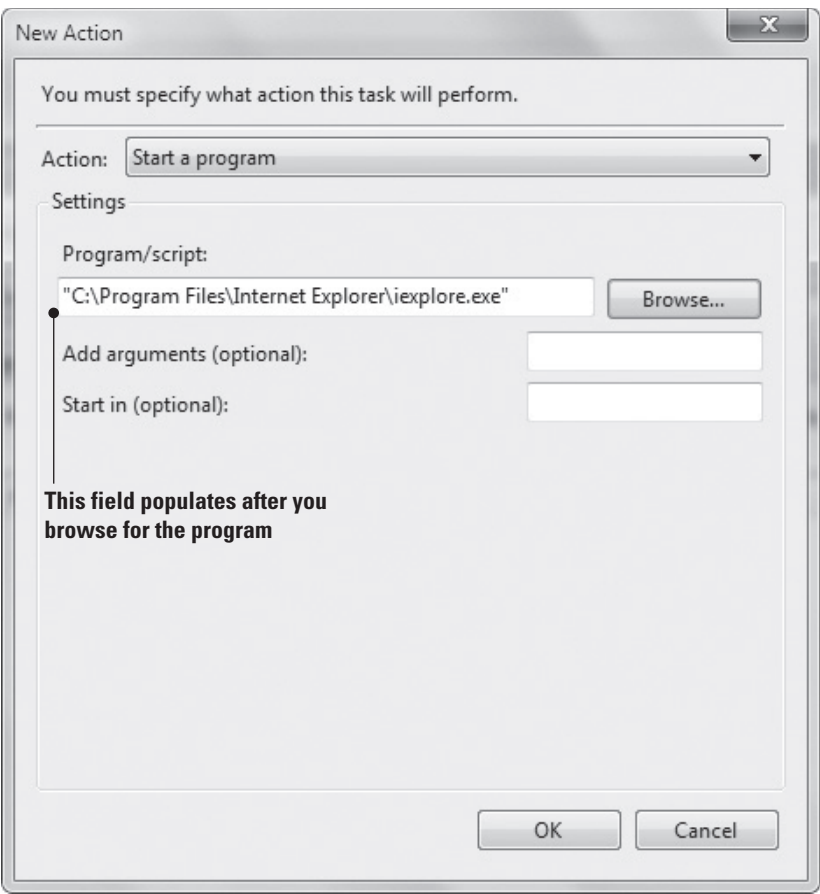
4. In the Create Task dialog box, click the **Actions** tab, and then click **New**. In the New Action dialog box, click **Browse**, navigate to the program's executable file (in this example, navigate to C:\Program Files\Internet Explorer\ and locate the Internet Explorer 9 executable named iexplore.exe), select it, and then click **Open**. The New Action dialog box should look similar to Figure 7-18.
5. Click **OK**.
6. In the Create Task dialog box, click the **Conditions** tab. In addition to the trigger, you can specify conditions under which the task should run (see Figure 7-19). For example, the power conditions are selected in an effort to avoid running a laptop's battery down unnecessarily. Make selections as appropriate.
7. Click the **Settings** tab. Here you can control task behavior (such as whether the user should be able to run the task on demand), how often the task should attempt to restart if it fails, and so on. Make selections as appropriate.
8. When you're finished configuring settings, click **OK**.

TAKE NOTE *

To delete a task from Task Scheduler, double-click it in the Active Tasks pane and click Delete in the Action pane.

Figure 7-18

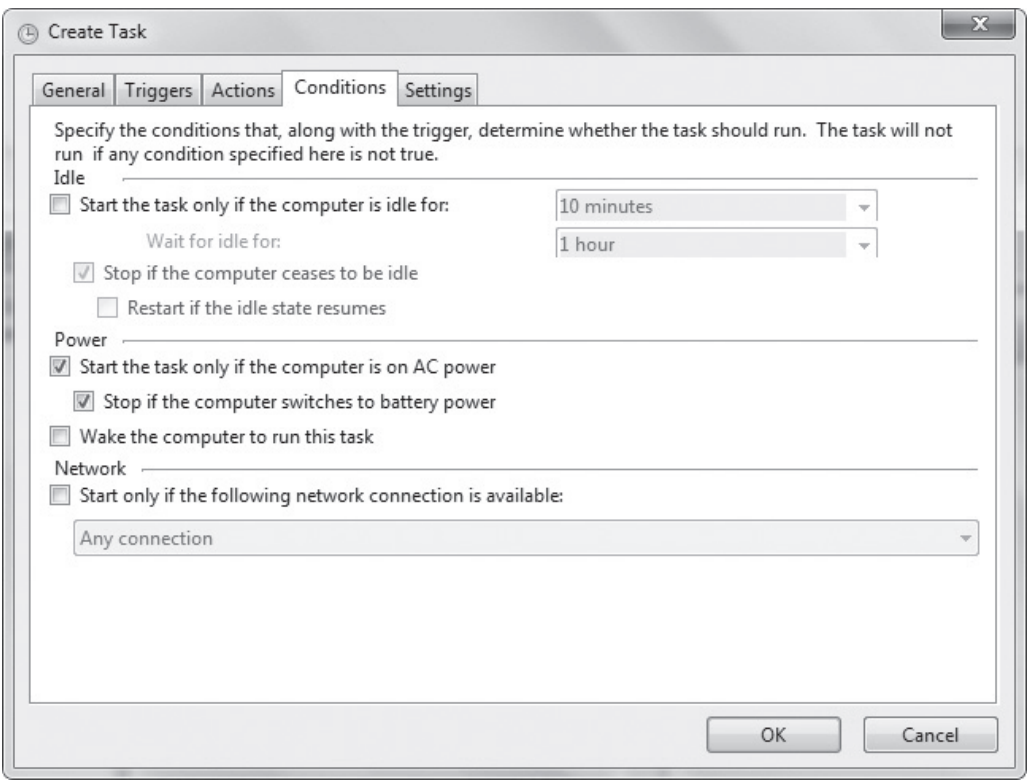
The New Action dialog box after selecting the program to run



This field populates after you browse for the program

Figure 7-19

Selecting conditions for the new task



The task is added to Task Scheduler. You can see the task listed in the Active Tasks pane at the bottom of the main Task Scheduler window.

+ MORE INFORMATION

To learn more about scheduling tasks in Windows 7, visit <http://windows.microsoft.com/en-US/windows7/schedule-a-task>

Understanding Action Center

Windows 7 Action Center is an improvement upon Security Center in previous versions of Windows. Within Action Center, you can view the status of security features (firewall, antivirus software, etc.) and maintenance (backups, updates, etc.).

CERTIFICATION READY

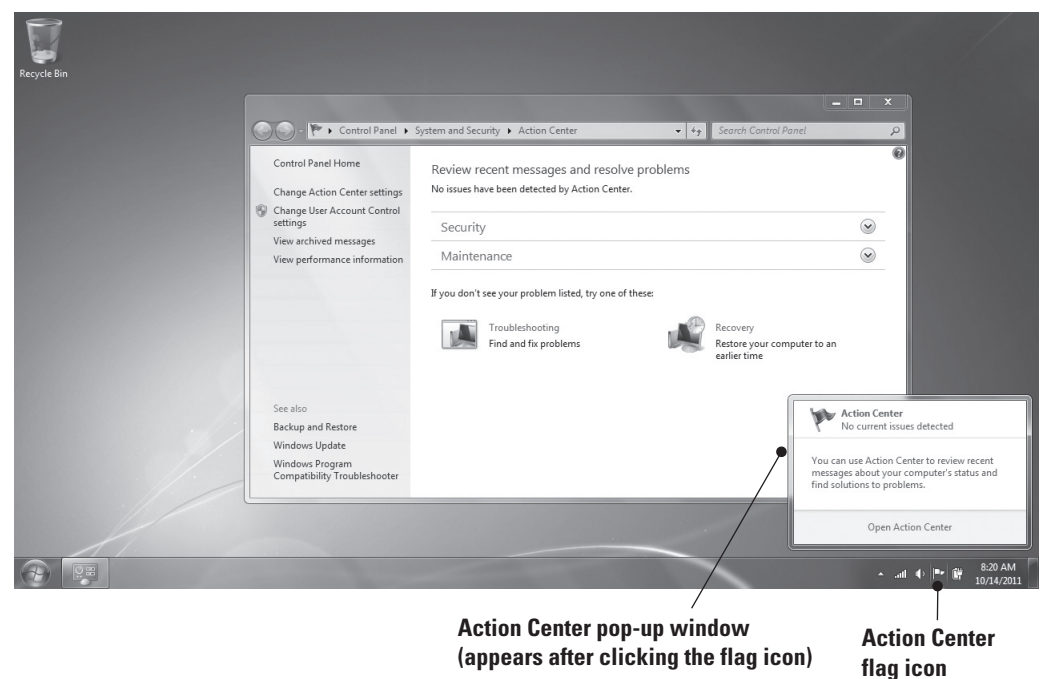
How can Action Center help you to maintain a computer?

6.2

Action Center provides a single interface in which you can view the status of security and maintenance features (see Figure 7-20) and it alerts you to problems you need to correct and usually provides a way to fix it. (You'll learn about the security features of Action Center later in this lesson.)

Figure 7-20

Action Center



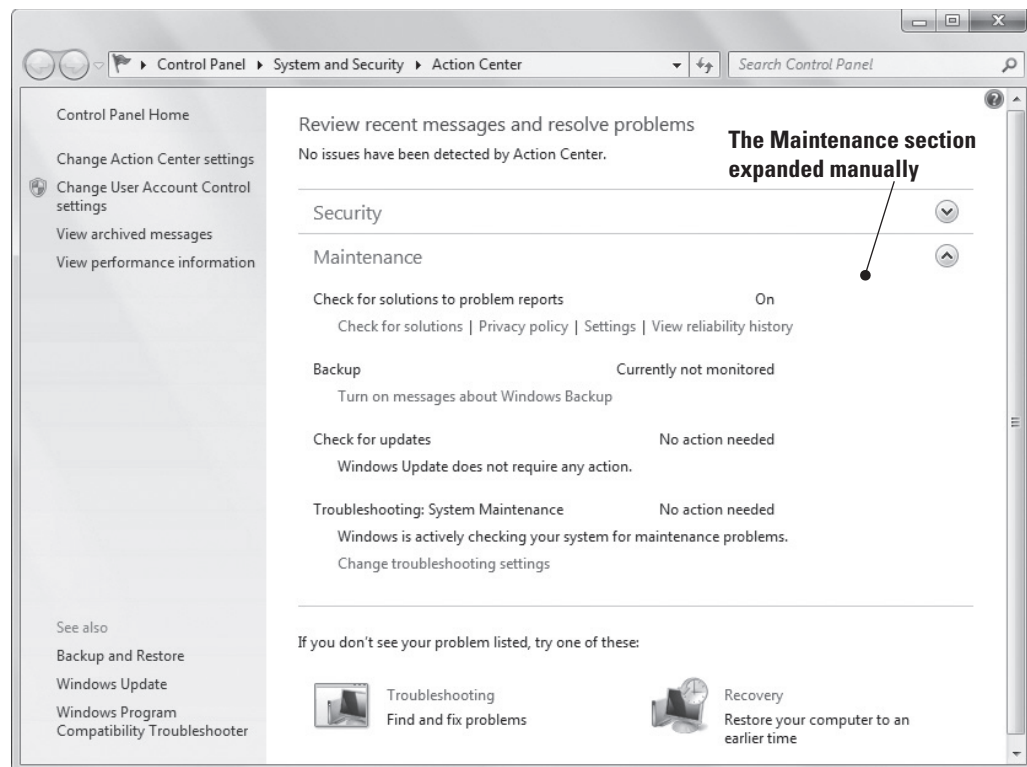
The quickest way to open Action Center is from the desktop. Click the flag icon in the notification area of the taskbar icon, and then click Open Action Center in the pop-up window. If no issues are pending, both the Security section and the Maintenance section are collapsed. When an issue needs your attention, one or both sections are expanded and the problem is described. Items can be displayed with yellow or red bars. A yellow bar indicates a suggested change; a red bar indicates a change that should be taken care of immediately.

In the expanded Maintenance section (see Figure 7-21), Action Center tracks four features:

- **Check for solutions to problem reports:** From here you can check for solutions, view the Windows 7 privacy policy, change settings to choose how often to check for solutions to problems reports, and view a graph of the system's reliability history.
- **Backup:** This section provides information about the status of Windows Backup on your computer. You'll learn about Windows Backup in Lesson 8.
- **Check for updates:** This section refers to Windows Update, which provides updates to the operating system and many installed programs. You'll learn about Windows Update later in this lesson.
- **Troubleshooting: System Maintenance:** This section displays messages related to the automatic troubleshooting feature in Windows 7, which actively monitors your system for any maintenance issues.

Figure 7-21

Action Center Maintenance section



You might not need to visit Action Center very often; you might need to visit only when an issue occurs. Windows 7 notifies you of any pending issues by displaying a red X under the flag in the notification area.

+ MORE INFORMATION

For details about Action Center in Windows 7, visit <http://windows.microsoft.com/en-US/windows7/What-is-Action-Center>

Understanding System Information

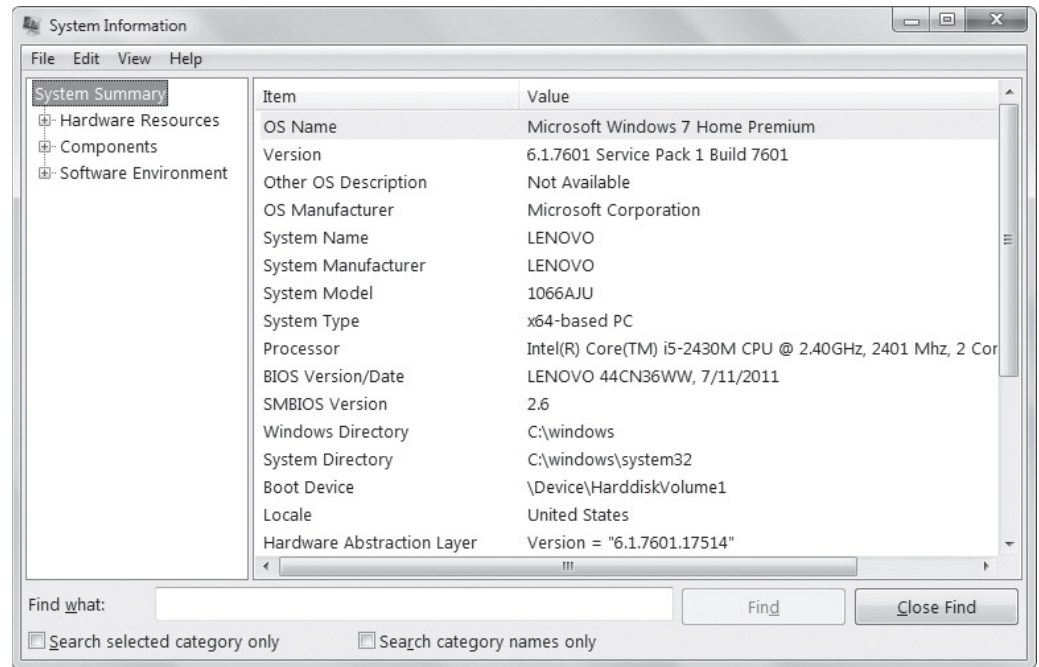
System Information displays a wealth of information about your computer's hardware, drivers, and system software. If you're having any type of system-related issues, you should check System Information for possible clues as to the source of the problem.

CERTIFICATION READY
What is the purpose of
System Information?
6.2

System Information is a utility that displays details about your computer's hardware components, software, and drivers. You can use System Information to simply gather information about your computer or to diagnose issues. To open System Information, click Start, type **system info** in the *Search programs and files* search box, and then select System Information in the resulting list. The main System Information window is shown in Figure 7-22.

Figure 7-22

The System Information window



The left pane includes the following categories:

- **System Summary:** This category displays general information about your computer. You can view the name of the operating system, the name of the computer (system), the type of processor, and much more.
- **Hardware Resources:** This category displays details about your computer's hardware, such as whether any conflicts exist and the status of input/output (I/O) devices.
- **Components:** This category displays information about hardware devices and their drivers, such as disk drives, network adapters, and computer ports.
- **Software Environment:** This category displays details about system drivers, current print jobs and network connections, services, startup programs, and other system-related items.

System Information provides a search feature that enables you to quickly find specific information about your system. Just type the information you're looking for in the Find what box at the bottom of the window. For example, to see which programs launch at startup, type **startup** in the Find what box and then click Find. You can narrow your search by selecting either the *Search selected category only* or *Search category names only* check boxes at the bottom of the System Information window.

When attempting to diagnose a system problem, it can be useful to export information in System Information to a text file to send to a fellow support technician or post on a troubleshooting forum on a Web site. System Information enables you to save information to an .nfo file format, which you can open from System Information, or export information to a standard text file with a .txt file extension.

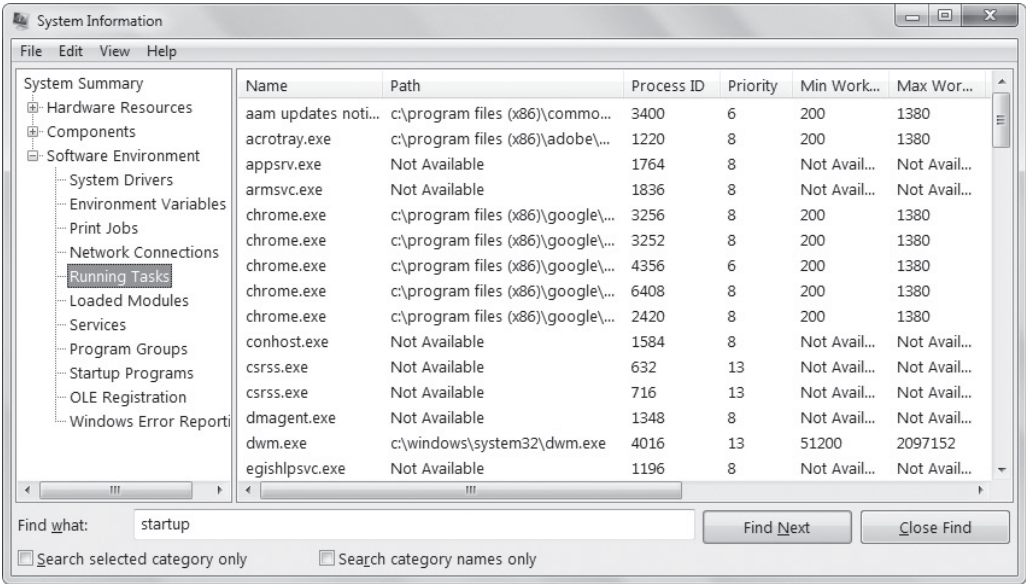


SAVE SYSTEM INFORMATION TO A TEXT FILE

GET READY. To save System Information to a text file, perform the following steps:

- 1. Click **Start**, type **system info** in the **Search programs and files** search box, and then select **System Information** in the resulting list.
- 2. In the System Information Windows, click **File > Export**.
- 3. Type a name for the file, and then click **Save**. The resulting file is very long and contains all of the information collected by System Information.
- 4. To export specific information from System Information, such as the list of currently running tasks, expand the **Software Environment** category in the left pane and select **Running Tasks** (see Figure 7-23).

Figure 7-23
Selecting specific information to export to a text file



- 5. Click **File > Export**, type a name for the file, and then click **Save**.

You can open the text files in Notepad, WordPad, or any word processing program.

+ MORE INFORMATION

For details about the System Information utility in Windows 7, visit <http://windows.microsoft.com/en-US/windows7/What-is-System-Information>

■ **Maintaining the Windows Registry**



THE BOTTOM LINE

The Windows registry is a database of configuration settings for your computer. It's often referred to as the "brains" of a Windows operating system. The registry is self-sufficient and rarely requires maintenance, but you can use a reputable registry cleaner occasionally to remove settings that are no longer used.

The **Windows registry** is a database in Windows that stores user preferences, file locations, program configuration settings, startup information, hardware settings, and more. In addition, the registry stores the associations between file types and the applications that use

CERTIFICATION READY

What is the purpose of the Windows registry?

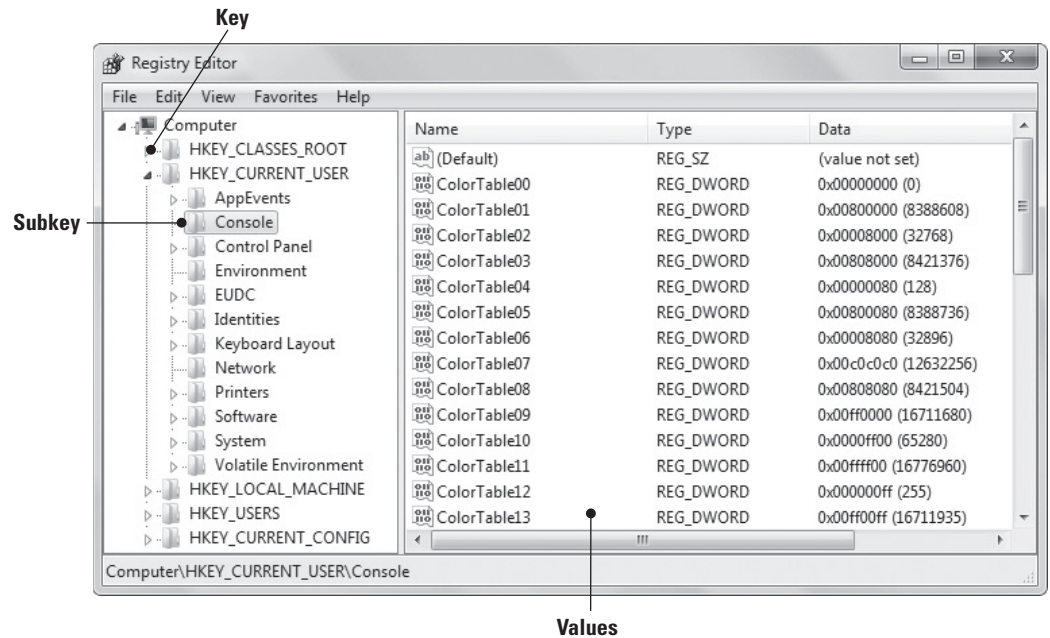
3.3

them. For example, the registry holds the information that tells Windows to open the default media player program (usually Windows Media Player) when you double-click a music or movie file.

The registry is made up of keys, subkeys, and values, as shown in Figure 7-24. Registry keys are similar to folders in Windows Explorer in that the keys can have subkeys (like subfolders). Subkeys have values that make up the preferences, configuration settings, and so on of the operating system. Whenever you change a preference, install software or hardware, or essentially make any changes to the system, the changes are reflected in the Windows registry.

Figure 7-24

A portion of the Windows registry



Over time, some settings in the registry are no longer needed. Registry settings take up a relatively small amount of disk space, and the settings can remain in the registry without affecting the performance of the computer. However, a registry setting can also become corrupt. Microsoft doesn't provide tools to repair the registry directly, but registry cleaners are available that remove unnecessary settings (for programs that are no longer installed, for example) and can repair many problems.

TAKE NOTE *

Some registry cleaners can actually harm your computer. Be sure to get a reputable program to avoid contaminating your PC with spyware and viruses.

You should back up your registry before running any maintenance program on it. Microsoft provides the Registry Editor utility to make changes to the registry and back it up. To open Registry Editor, click **Start** and in the *Search programs and files* search box, type **regedit**, and then select **regedit.exe** from the resulting list. The Registry Editor window displays, which should look similar to Figure 7-24 shown previously.

Only users with advanced computer skills and IT professionals should edit the registry. Changing or deleting a critical setting can prevent your computer from operating upon reboot. However, nearly anyone can safely back up the registry.



BROWSE AND BACK UP THE WINDOWS REGISTRY

GET READY. To browse and then back up the Windows registry, perform the following steps:

1. Open Registry Editor by clicking **Start**, typing **regedit** in the **Search programs and files** search box, and selecting **regedit.exe** from the resulting list.
2. Expand keys in the left pane to view the associated subkeys. To view Microsoft-related subkeys, for example, click the clear triangle to the left of **HKEY_CURRENT_USER** key, click the **Software** subkey, and then click the **Microsoft** subkey. Browse the list of Microsoft subkeys.
3. Similarly, expand the **HKEY_LOCAL_MACHINE** key, expand the **SOFTWARE** subkey, and then expand the **Microsoft** subkey. Another set of Microsoft-related subkeys displays.
4. Collapse (close up) all keys by clicking the black triangles to the left of each expanded entry in the left pane.
5. Click **File > Export**, navigate to the location where you want to save the registry backup file, type a name for the backup in the **File name** text box, and then click **Save**.

A best practice is to save registry backups to an external location, such as a USB flash drive, a CD/DVD, or a network drive.

■ Updating the System



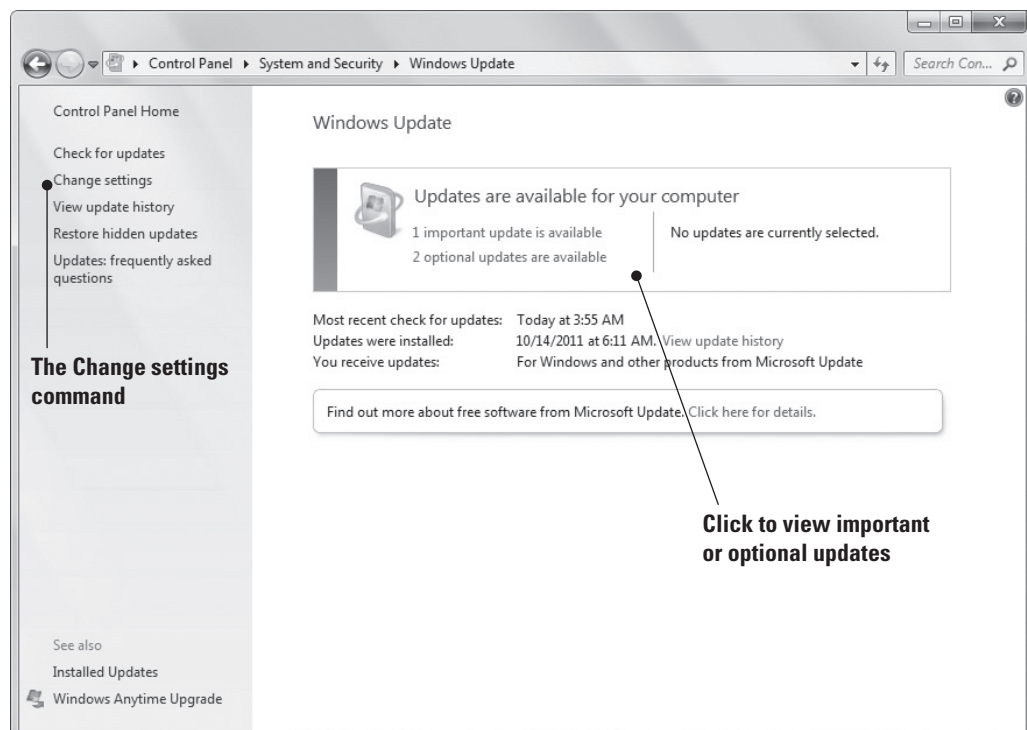
THE BOTTOM LINE

Microsoft provides several ways to help you keep your Windows system patched and updated using hotfixes, service packs, updated drivers, and more. Windows Update and Microsoft Update are the primary update tools.

Keeping a Windows system patched and updated is vitally important to maintaining proper security. Microsoft provides regularly scheduled updates via the **Windows Update** feature (see Figure 7-25), along with critical updates as they come up.

Figure 7-25

The Windows Update window

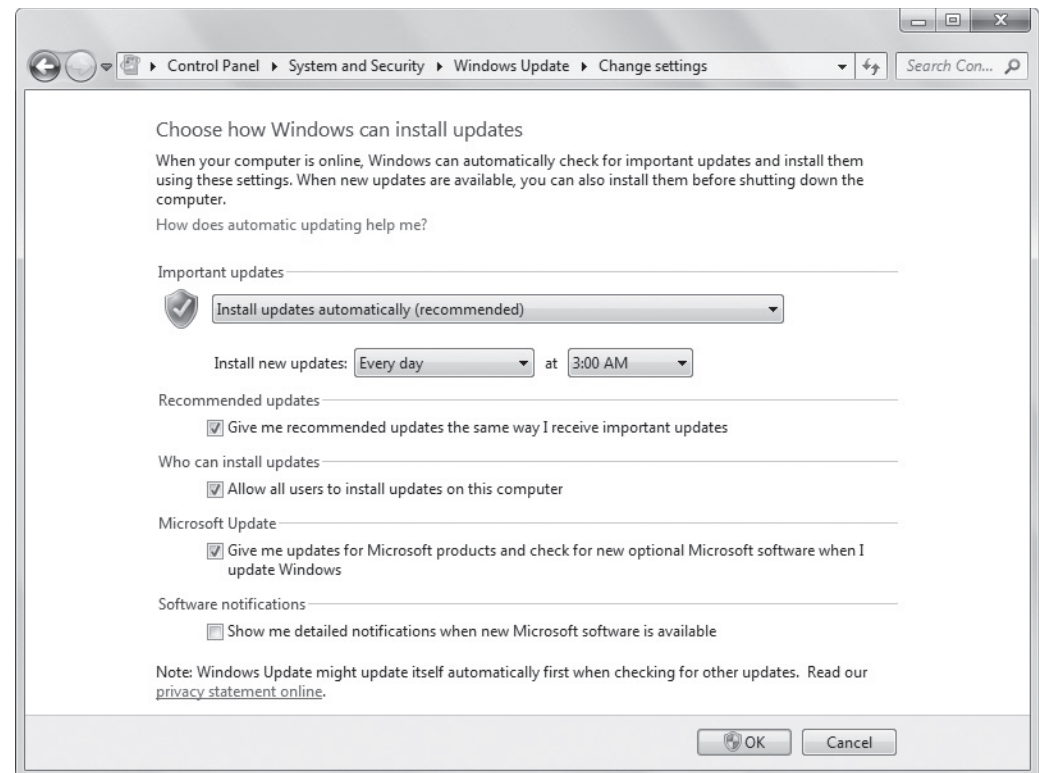


Microsoft releases regular, critical updates usually on the second Tuesday of the month (referred to as Patch Tuesday), although the company might release them more often to fix serious security vulnerabilities. These updates install automatically if you have automatic updating turned on.

To check your Windows Update settings, click the *Change settings* command in the task pane of the Windows Update page. The Change settings page (see Figure 7-26) allows you to choose whether you want to receive updates automatically (recommended) or per your own schedule. If you want Windows Update to download updates but let you choose which ones to install, or have Windows Update check for updates and let you choose which ones to download and install, click the *Important updates* drop-down arrow and select your preferred option.

Figure 7-26

The Change settings page



CERTIFICATION READY

What are the three main types of updates installed by Windows Updates?

6.3

CERTIFICATION READY

How do Windows Update and Microsoft Update deliver updates to Windows computers?

6.3

CERTIFICATION READY

What is a hotfix?

6.3

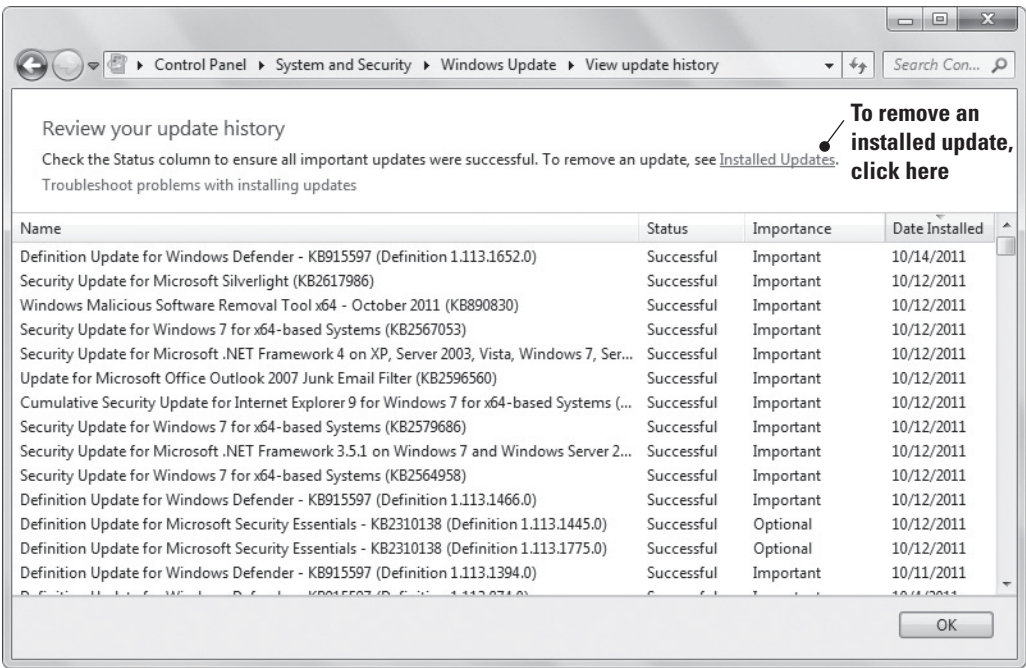
On the Change settings page, notice the **Microsoft Update** option. When this option is selected, Microsoft delivers updates for additional Microsoft software, not just the Windows operating system.

You view all of the updates that have been applied to your computer by returning to the main Windows Update page and clicking the *View update history* command in the task pane. The View update history window (see Figure 7-27) shows the name of each update, whether it installed successfully or not, the type of update (Important, Recommended, or Optional), and the date installed. Double-click any update to get more information.

Even with automatic updates enabled, some updates are not installed automatically; Microsoft gives you the option to install them. To view these updates, click one of the links in the Updates are available for your computer section of the Windows Update window. Windows Update pushes three types of updates to your computer:

- **Important updates:** These include security and critical updates, hotfixes, service packs, and reliability improvements. A **hotfix** is a patch that typically fixes a bug in software. If the bug creates a security issue or results in a part of the software malfunctioning,

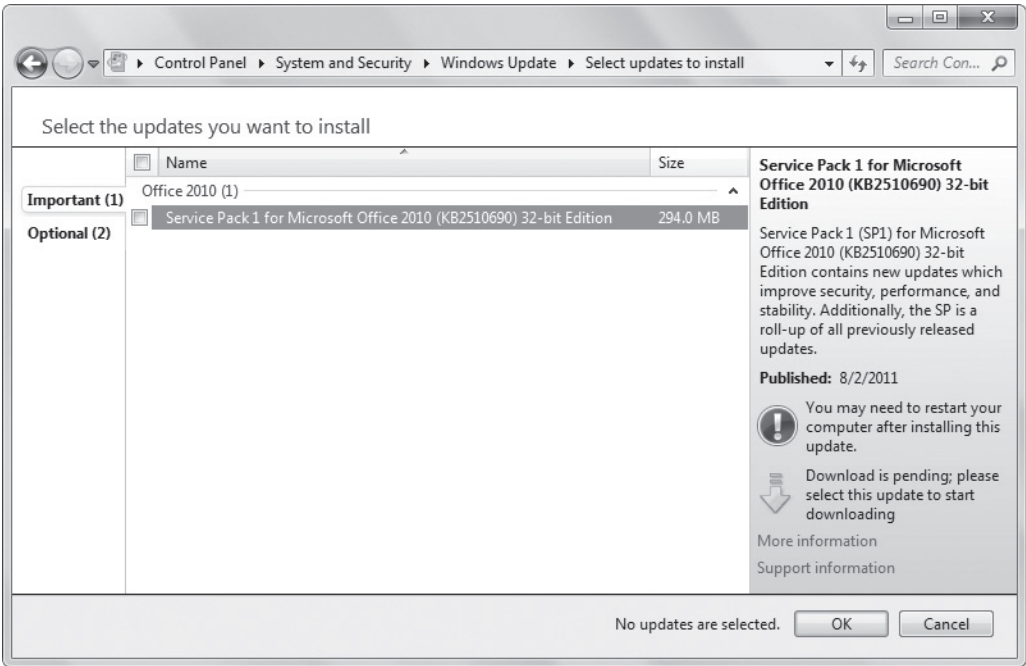
Figure 7-27
Viewing the Windows Update history



the manufacturer usually distributes a hotfix soon after the bug is detected. A Windows *service pack* is a collection of updates and hotfixes since the product was released. The product might be the operating system or Microsoft software. Figure 7-28 shows an example of an important update.

- **Recommended updates:** These include software updates and new or improved features to help keep your operating system and software running optimally.

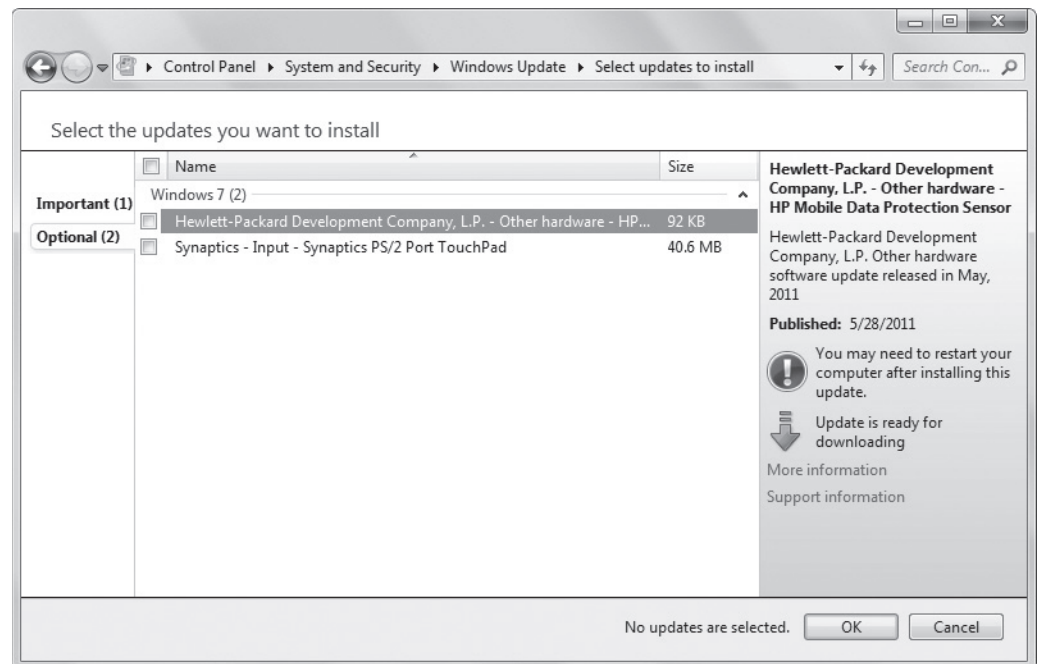
Figure 7-28
An example of an important update



- **Optional updates:** These include items such as optional device drivers for components on your computer, or new or trial Microsoft software. Figure 7-29 shows an example of optional updates (in this case, device drivers).

Figure 7-29

An example of optional updates



To install any of these updates, select the box next to the name of the update and then click OK. Many updates require you to restart your computer for the update to take effect. You can usually continue working and then restart when it's convenient. However, it's best to restart immediately if one or more critical updates have been installed.

Administrators in all but very small environments often use Windows Server Update Services (WSUS) to gather Windows updates and hotfixes and then distribute them to client computers. WSUS runs on a Windows server. The service downloads updates and hotfixes to the server, allowing the administrator to install them on test computers that are configured similar to actual user computers. If the tests do not result in any problems, the administrator approves the updates or hotfixes, and WSUS then installs them on client computers over the network.

+ MORE INFORMATION

For more information about Windows Update, visit <http://windows.microsoft.com/en-US/windows7/products/features/windows-update>. To learn about the Microsoft update management process, go to <http://technet.microsoft.com/en-us/library/cc700845.aspx>

■ Defending Your System from Malicious Software

↓ THE BOTTOM LINE

One of the most challenging problems for computer users and administrators is to prevent viruses, worms, and other types of malware from infecting your computer. The Windows 7 Action Center: Security section helps you manage your computer's security. Microsoft Windows Defender and Microsoft Security Essentials help to prevent spyware and malware infections, respectively.

With thousands of different viruses, worms, and other forms of *malicious software (malware)* ready to attack any computer connected to the Internet, it's vitally important to use antivirus and antispyware software in addition to a firewall.

Many protection companies sell stand-alone antivirus, antispyware, and firewall programs that are bundled into Internet security products that usually provide additional features (such as antispam and anti-phishing filters, parental controls, and password vaults). At a minimum, every computer should have antivirus and antispyware software installed along with a firewall; every computer should also use the security settings found in the latest Web browsers.

The following sections review tools available in Windows 7 and downloadable from the Microsoft Web site that enable you to protect your computer from malware.

Understanding Action Center

The Security section of Action Center lets you view the status of many different security features and fix security vulnerabilities if any are present.

CERTIFICATION READY

How does the Action Center help to protect a computer?

3.3

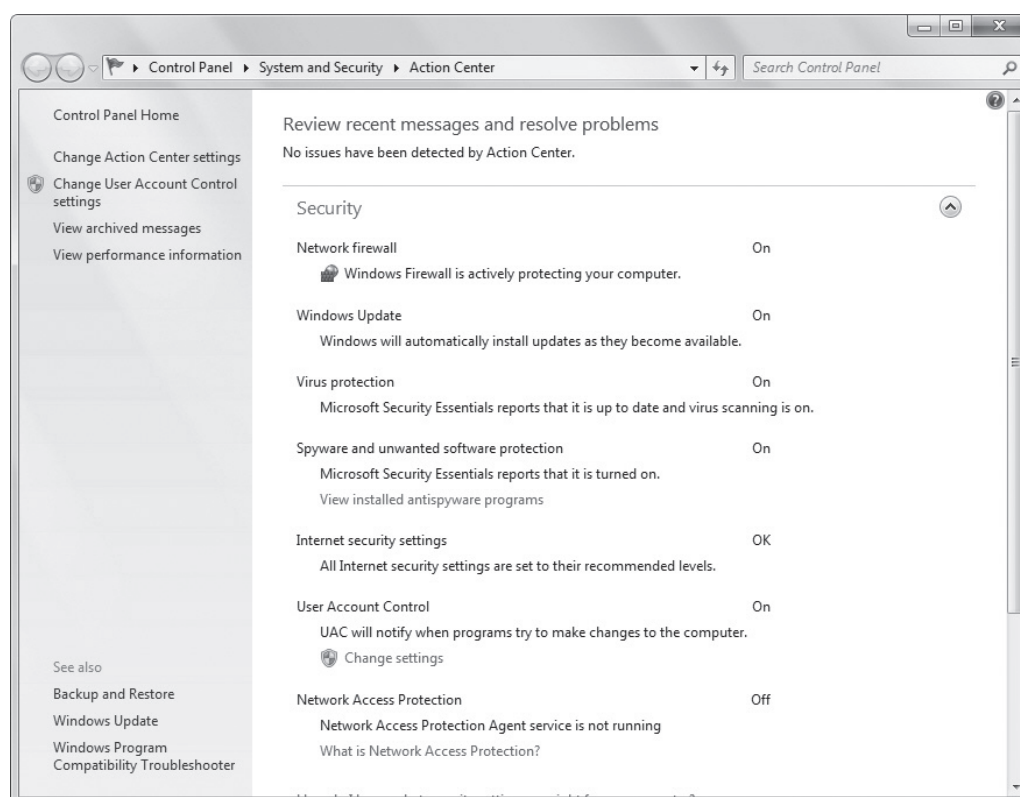
You learned the essentials of Action Center earlier in this lesson. Although Action Center provides some information regarding maintenance, it really shines on security issues. And it should—Action Center is the new and improved version of the Windows Security Center that was featured in Windows XP SP2 and Windows Vista.

By default, Action Center tracks seven security features (see Figure 7-30):

- **Network firewall:** This feature monitors your computer's firewall, through which network and Internet traffic flows. Windows 7 comes with Windows Firewall, which should be turned on if no other firewalls are present.

Figure 7-30

Action Center's Security section



- **Windows Update:** This feature indicates whether Windows Update is enabled.
- **Virus protection:** Virus protection software installed on your computer is monitored with this feature. If no software is present or if it's out of date, you'll be notified here.
- **Spyware and unwanted software protection:** Action Center monitors Windows Defender (which comes bundled with Windows 7, and which you'll learn about shortly) and other third-party antispware solutions.
- **Internet security settings:** These settings are configured through the Security tab in Internet Explorer 9's Internet Options dialog box. You learned about Internet Explorer security zones in Lesson 3. If any zone is configured so that it poses a threat to your computer, you'll be notified here.
- **User Account Control:** In this section, you can see whether User Account Control (UAC) is enabled and you can click the Change settings link to configure it.
- **Network Access Protection (NAP):** This feature applies mainly to enterprise environments. With NAP enabled, the network can detect whether the computer meets baseline security standards for the organization. If not, the computer is not allowed access to the full network and must be updated or reconfigured before access is granted.

If any of these features require your attention, the Action Center flag in the notification area displays a red X. Click the flag to open Action Center and address important security issues. Important items that need your attention are designated with red bars.

Understanding Windows Firewall

Windows Firewall comes with Windows 7 and other Windows versions to protect your computer from traffic entering through communications ports.

TAKE NOTE *

Networks have firewalls, too—similar to computers but usually much more robust.

A **firewall** is a software program or device that monitors traffic entering and leaving a computer. This term comes from the building trades where it refers to a special barrier designed to delay the advance of fire from one area to another. In the computer world, threats and attacks are the “fire” advancing on computers connected to the Internet and from malicious insiders.

Microsoft provides **Windows Firewall** with Windows 7, Windows Vista, and Windows XP operating systems. The firewall is turned on automatically in new installations of the operating systems. To access Windows Firewall, click Start and in the *Search programs and files* search box, type **firewall**, and then select Windows Firewall from the resulting list. The Windows Firewall page displays whether the program is enabled (see Figure 7-31) and what it's protecting.

Sometimes a firewall works too well, blocking communications that you want to allow! For example, a newly installed program that needs to communicate with the Internet might not work because it's blocked by the firewall. In this case, click the *Allow a program or feature through Windows Firewall* command in the task pane of the Windows Firewall page. The Allowed Programs page displays (see Figure 7-32). To change settings, click the *Change settings* button. Click the *Allow another program* button. Scroll the list to locate the program, select it, click Add, and then click OK.

It's best to have only one firewall running on a computer. If you install an Internet security product, the new software should automatically turn off Windows Firewall. If you check Action Center and see that two firewalls are running, open the Windows Firewall page, click *Turn Windows Firewall on or off* in the task pane, select the *Turn off Windows Firewall* option, and then click OK. Reboot your computer, and then immediately check Action Center again to verify that only one firewall is enabled.

Figure 7-31
The Windows Firewall page

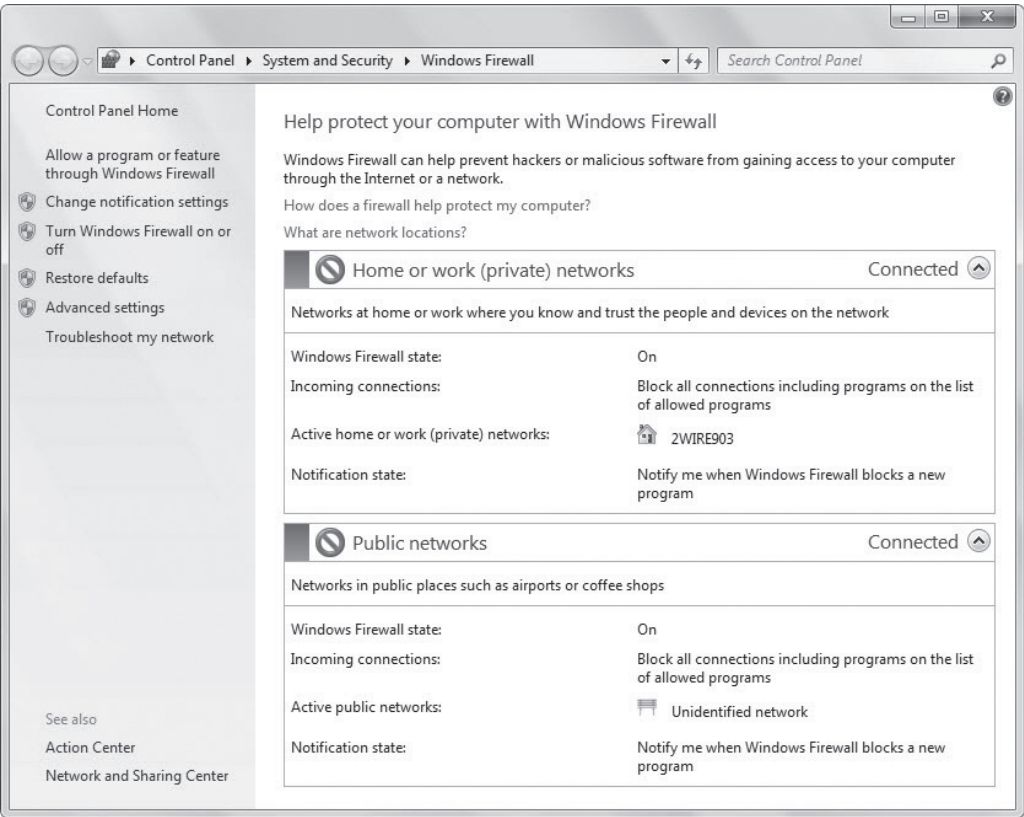
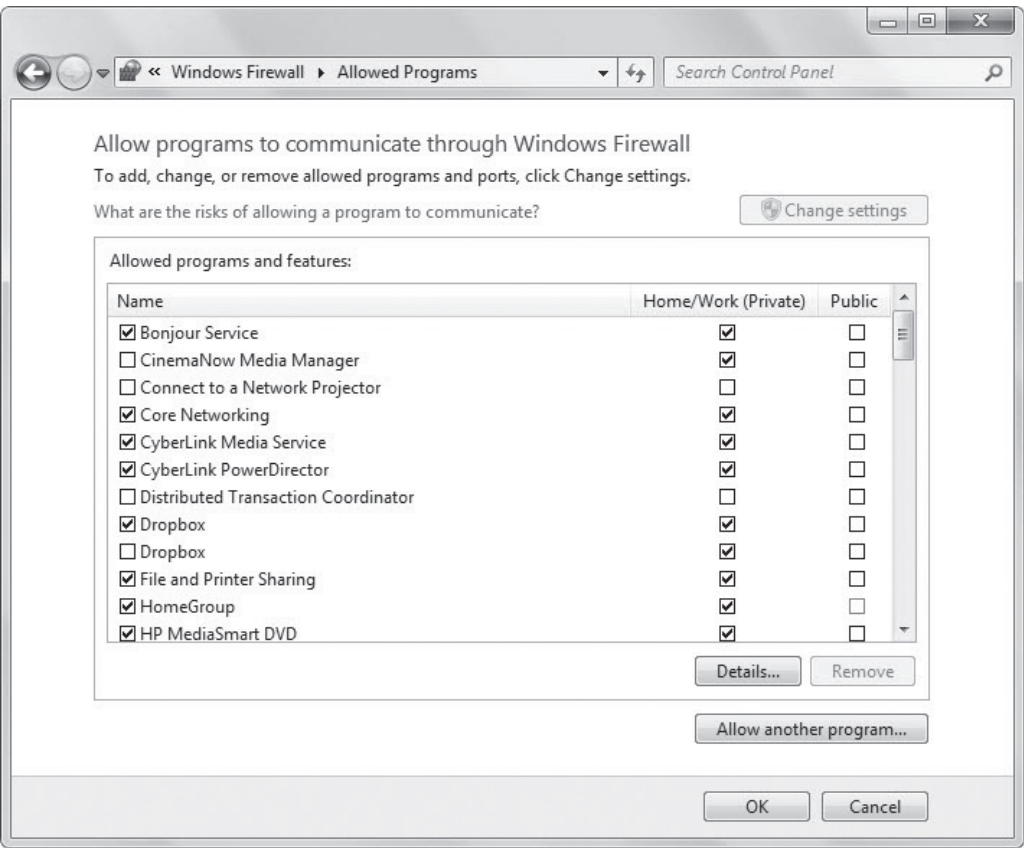


Figure 7-32
The Windows Firewall Allowed Programs page



Understanding Windows Defender

Windows Defender is a free software program that provides antispyware protection for a Windows computer.

CERTIFICATION READY

How does Windows Defender help protect your system?

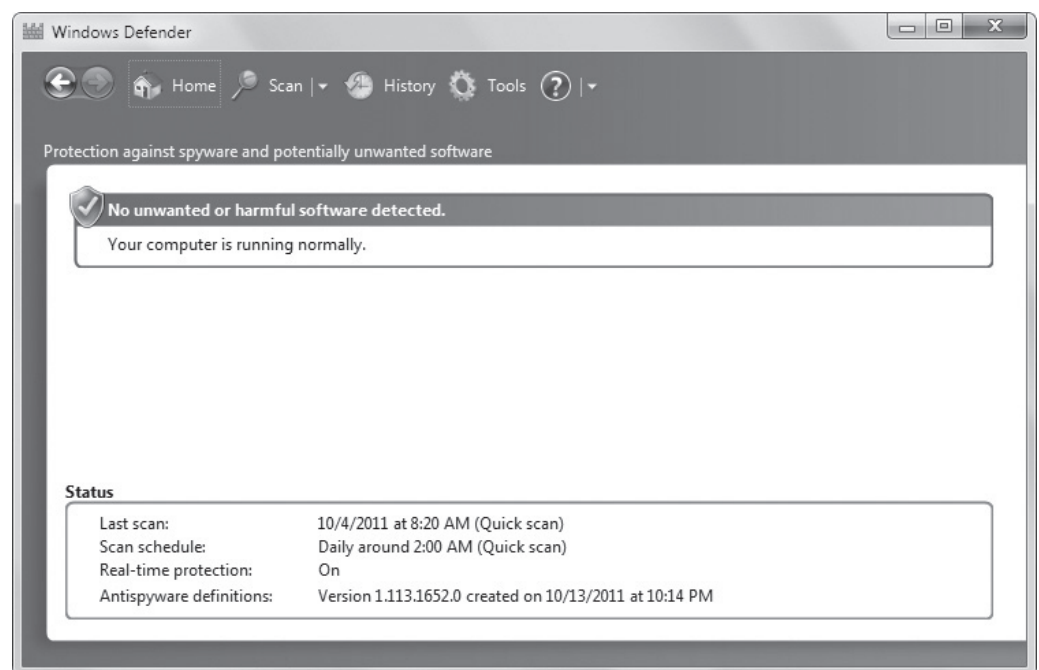
3.3

Spyware is a type of program that installs on your computer without your permission, monitors your computing activities, and reports the activity back to the spyware writer or a third party. Some legitimate companies use spyware to gather profile information about their customers for direct marketing and product development efforts; however, most spyware is malicious in nature.

A free antispyware program provided by Microsoft is **Windows Defender**, which comes bundled with Windows 7. The Windows Defender window is shown in Figure 7-33. You can set Windows Defender to run in the background, constantly monitoring your computer for spyware. When it detects spyware, the program quarantines it (so the spyware can't run on your computer) or deletes it. Quarantining is handy in case Windows Defender mistakenly deems a "good" program as spyware; by only quarantining it, you're provided with an opportunity to restore the program.

Figure 7-33

The Windows Defender main page

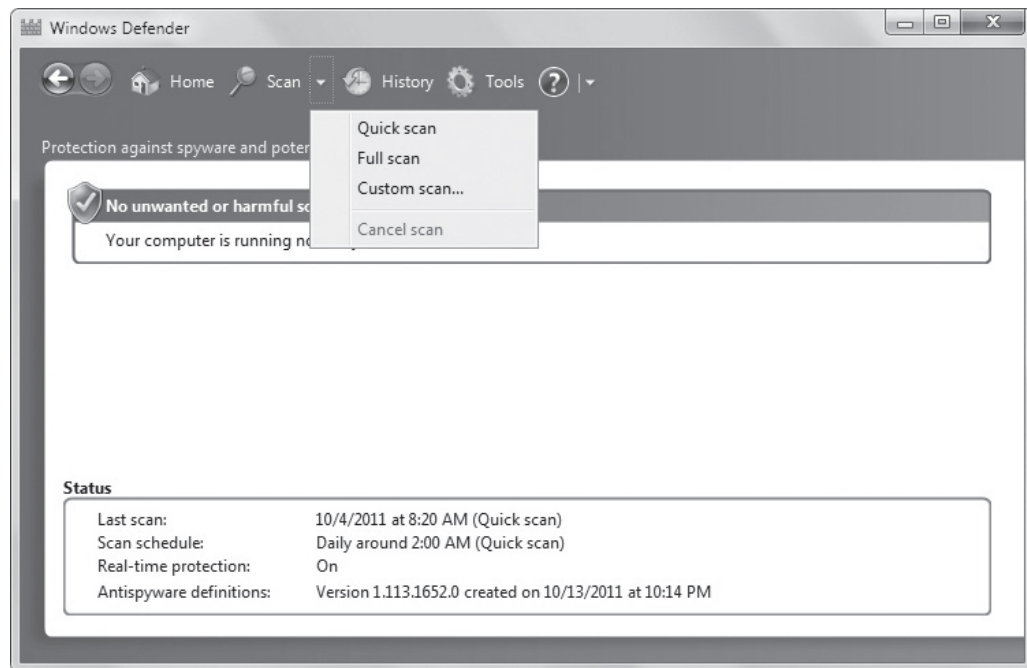


To open Windows Defender, click Start, type **defender** in the *Search programs and files* search box, and then select Windows Defender from the resulting list. If Windows Defender is not already running, click the link in the pop-up box that displays to enable Windows Defender. You might have to start the service manually in the Services MMC snap-in, or you might have to restart your computer. If you have other anti-malware software running on your computer, such as the latest version of Microsoft Security Essentials (covered in the next section), Windows won't allow you to start Windows Defender.

To run a scan of your computer, click the down arrow next to the Scan icon at the top of the window (see Figure 7-34) and then select Quick scan, Full scan, or Custom scan.

Figure 7-34

Windows Defender's scanning options



A quick scan checks critical files and those most often affected by spyware. A full scan checks all files on your hard disk and can take several hours to complete, depending on the number of files on your computer. A custom scan lets you choose which files or folders to scan.

Windows Defender comes with several configurable options, such as scheduling, default behavior when a threat is detected, an exception list, and much more.



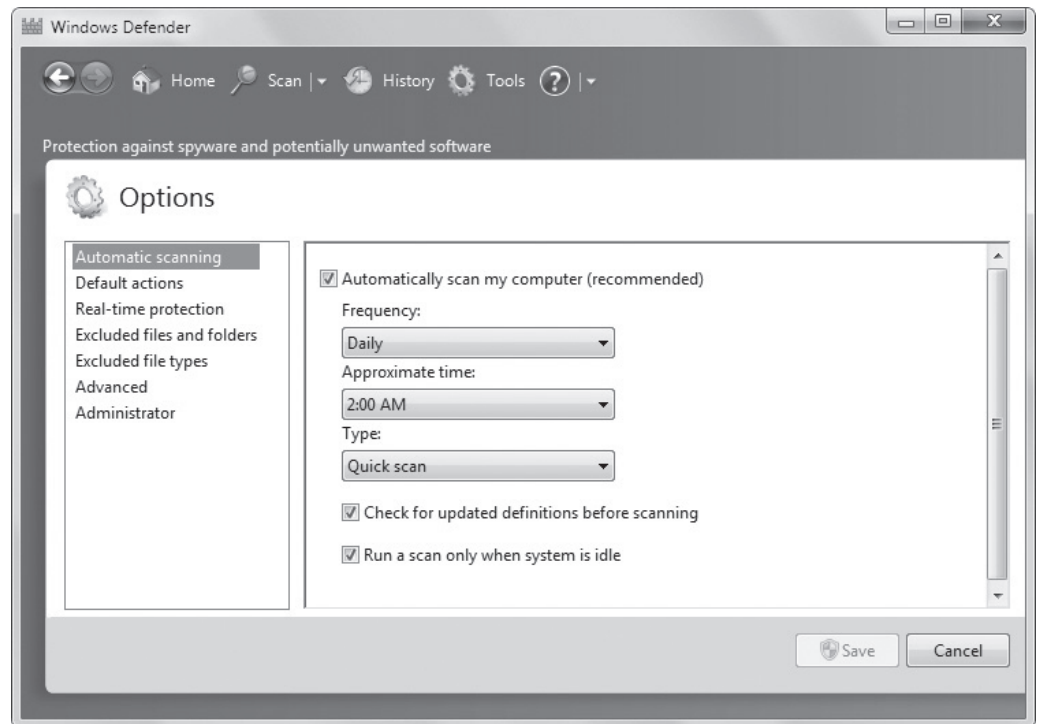
CONFIGURE WINDOWS DEFENDER

GET READY. To configure Windows Defender, perform the following steps:

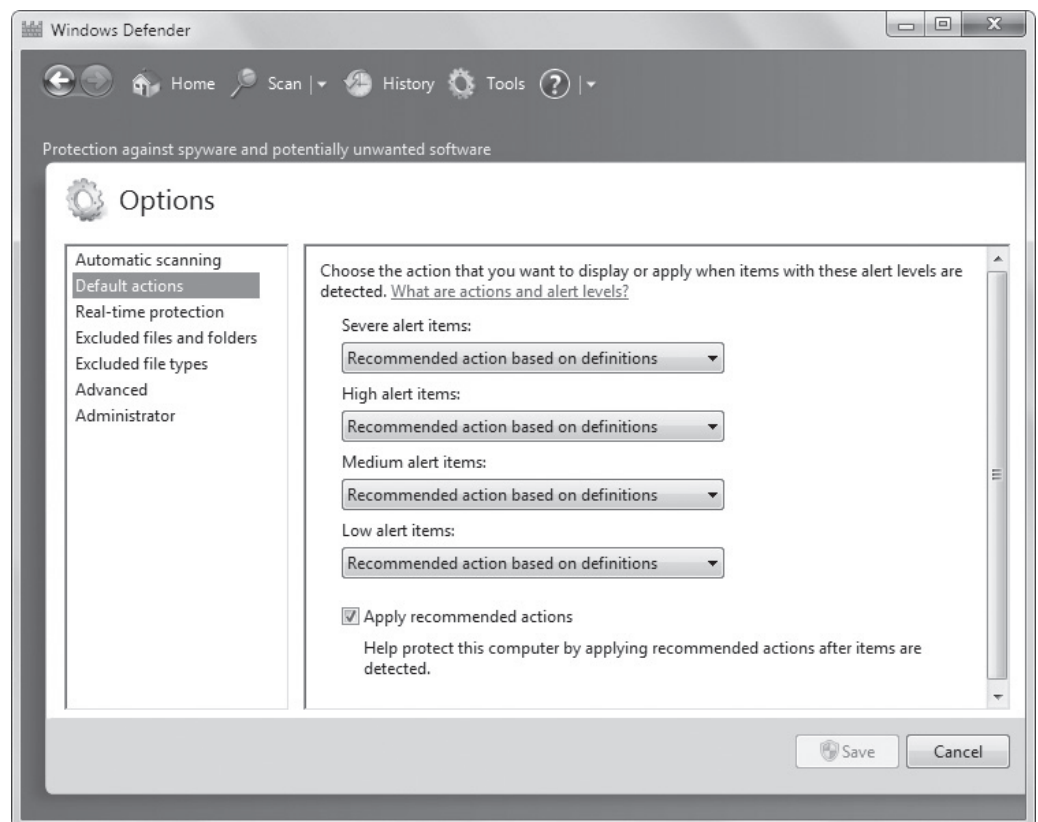
1. Click **Start > All Programs > Windows Defender**. Alternately, click **Start**, type **defender** in the **Search programs and files** search box, and then click **Windows Defender** in the resulting list.
2. In Windows Defender, click the **Tools** icon at the top of the window.
3. Click the **Options** link. The Options page displays (see Figure 7-35).
4. To change the automatic scanning schedule, click the drop-down lists and select a new frequency (either **Daily** or a particular day of the week), an **Approximate time**, and a **Type** of scan (**Quick** or **Full**).
5. In the left pane, click **Default actions**. You can set default behaviors when Windows Defender detects a severe, high, medium, or low alert item (see Figure 7-36). All options in the drop-down lists include the choice to **Quarantine** or to **Remove**. The medium and low alert levels also include the **Allow** option.
6. To exclude specific files or folders from the scans, click **Excluded files or folders** in the left pane, click the **Add** button, navigate to the file or folder you want to exclude, select it, and then click **OK**.
7. To exclude certain file types, click **Excluded file types** in the left pane. Type a file extension in the text box next to the Add button for the type of file that does not need to be scanned (such as *.jpg, *.tif, or *.pdf) and then click **Add**.

Figure 7-35

The Windows Defender Options page

**Figure 7-36**

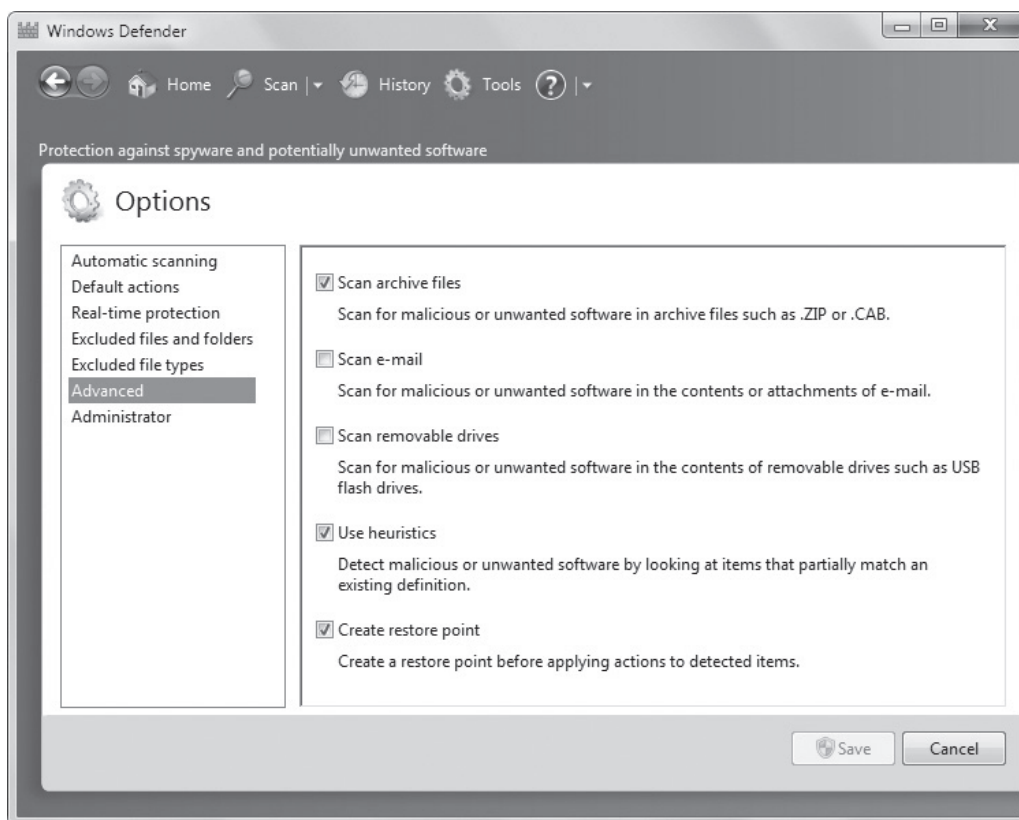
Setting default behaviors for alert levels



8. Click **Advanced** in the left pane. The advanced options (see Figure 7-37) include scanning archive files, scanning e-mail (including attachments), and scanning removable drives (such as a connected USB flash drive). You can also tell Windows Defender to use heuristics when scanning files; heuristics is a process or method that looks for partial matches to spyware rather than a complete match. This is a deeper form of scan that can catch more spyware. Finally, if Windows Defender must take action on a threat, such as removing it, the **Create restore point** option creates a restore point you can roll back to if needed. (Restore points are covered in Lesson 8.)

Figure 7-37

Setting advanced options



9. When you're finished configuring Windows Defender, click **Save**.

Windows Defender is a good antispymware program, but it doesn't protect you as well as a more feature-rich program such as Microsoft Security Essentials, which is covered in the next section.

+ MORE INFORMATION

You can learn more about Windows Defender by visiting <http://windows.microsoft.com/en-US/windows7/products/features/windows-defender>

Understanding Microsoft Security Essentials

Microsoft Security Essentials is a program that helps protect your computer from viruses and other malware. You can run Microsoft Security Essentials for free on up to 10 computers.

Windows 7 doesn't include antivirus software, but every computer that interacts with other computers or the Internet should have antivirus software installed. As previously mentioned in this section, you can buy and install third-party antivirus software or an Internet security suite. You can also use the free antivirus software provided by Microsoft: Microsoft Security Essentials.

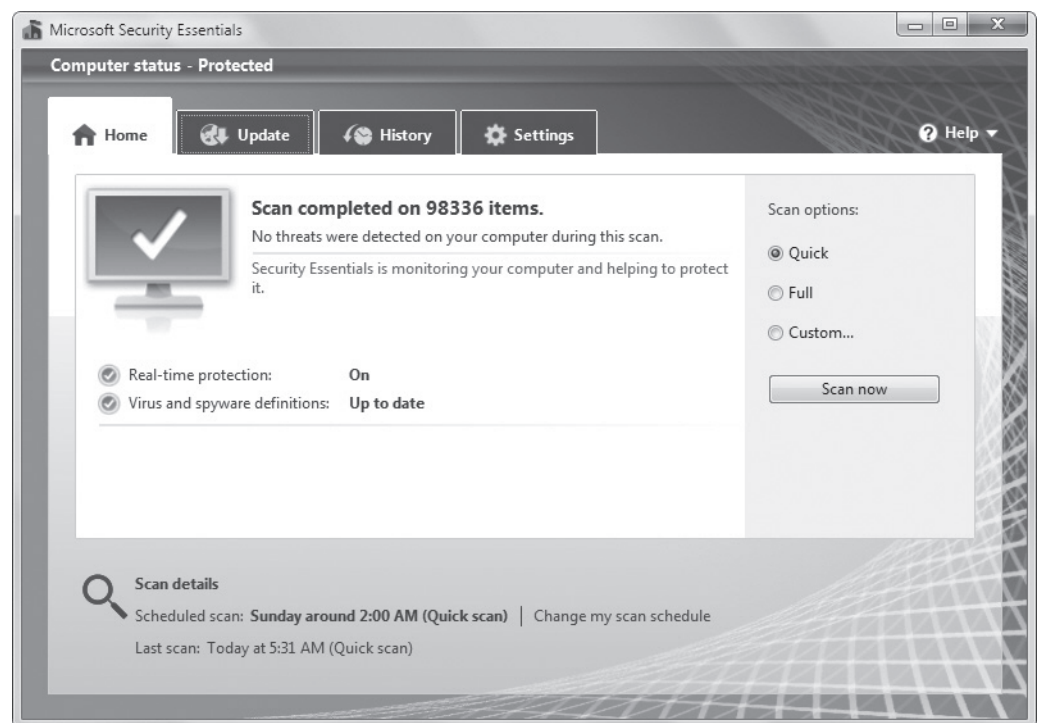
TAKE NOTE *

To download Microsoft Security Essentials, go to the Microsoft Security Essentials Web site or the Microsoft Download Center.

Microsoft Security Essentials (see Figure 7-38) protects your computer from viruses and many other forms of malware. The program is updated regularly by the Microsoft Update service to ensure the signatures, the anti-malware engine, and the application itself are kept up to date. A **signature** is a sequence of text or code that's programmed into a virus and uniquely identifies it. Antivirus software uses an anti-malware engine to find viruses and other malware on a computer. Because new threats appear every day, Security Essentials downloads new signatures daily and uses the Dynamic Signature Service to push the updates to your computer almost immediately.

Figure 7-38

The Microsoft Security Essentials main window



Like Windows Defender, Security Essentials offers three types of scans: quick, full, and custom. A quick scan checks critical files and those most often affected by spyware. A full scan checks all files on your hard disk and can take several hours to complete, depending on the number of files on your computer. A custom scan lets you choose which files or folders to scan. Just select the type of scan you want to run on the Home tab and then click *Scan now*.



INSTALL MICROSOFT SECURITY ESSENTIALS

GET READY. To install Microsoft Security Essentials, perform the following steps:

1. Download the Microsoft Security Essentials installation program to your hard disk, such as to your Downloads folder. The installation file is named `mseinstall.exe`. Don't disconnect from the Internet after downloading the file; you must be connected to the Internet to complete the installation of Microsoft Security Essentials.

TAKE NOTE *

You must be running a genuine version of Windows in order to install Microsoft Security Essentials. A genuine version of Windows is one that is published and licensed by Microsoft.

2. In Windows Explorer, locate and double-click **mseinstall.exe**. If prompted for administrative privileges, type the password or provide confirmation.
3. In the installation wizard, click **Next**.
4. Accept the license agreement and then click **Next**.
5. Choose or decline participation in the Customer Experience Improvement Program and then click **Next**.
6. Leave the **If no firewall is turned on, turn on Windows Firewall (Recommended)** option selected and then click **Next**.

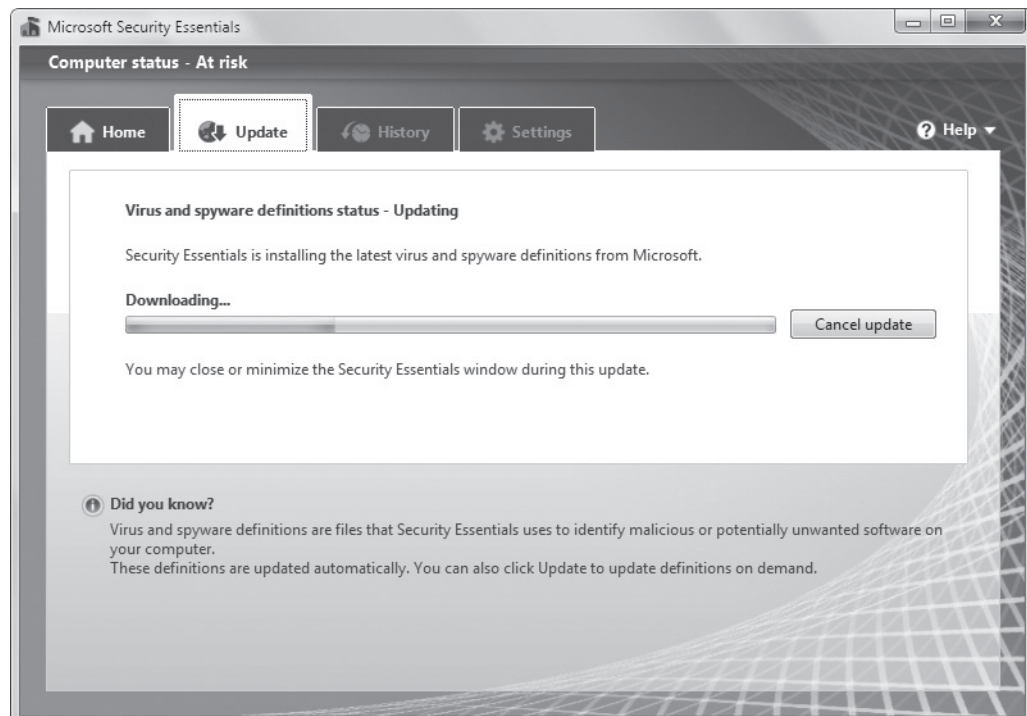
TAKE NOTE *

Making sure a firewall is enabled is highly important. You must have your computer connected to the Internet when installing Microsoft Security Essentials or the installation will fail. So, the firewall helps protect the computer for the short time that the computer is vulnerable to online attacks.

7. You're prompted to remove other antivirus software that might be installed on your computer before continuing.
 - If you need to remove the software, cancel the wizard, go to Control Panel, uninstall the program, and reboot your computer. Start from Step 2 in this exercise.
 - If no other antivirus software is installed, click **Install**.

Figure 7-39

The initial scan by Microsoft Security Essentials after installation



8. After the software installs, the final screen of the wizard provides the option to perform a system scan. Click **Finish**. The software immediately checks for updates for its definitions and signatures, and scans your system (see Figure 7-39). The red bar displayed at the top of the window indicates that the computer is at risk. Once the updates are installed, the status bar will change to green and indicate “protected.”

Your computer is now constantly monitored by Security Essentials, and offers real-time protection against malware.



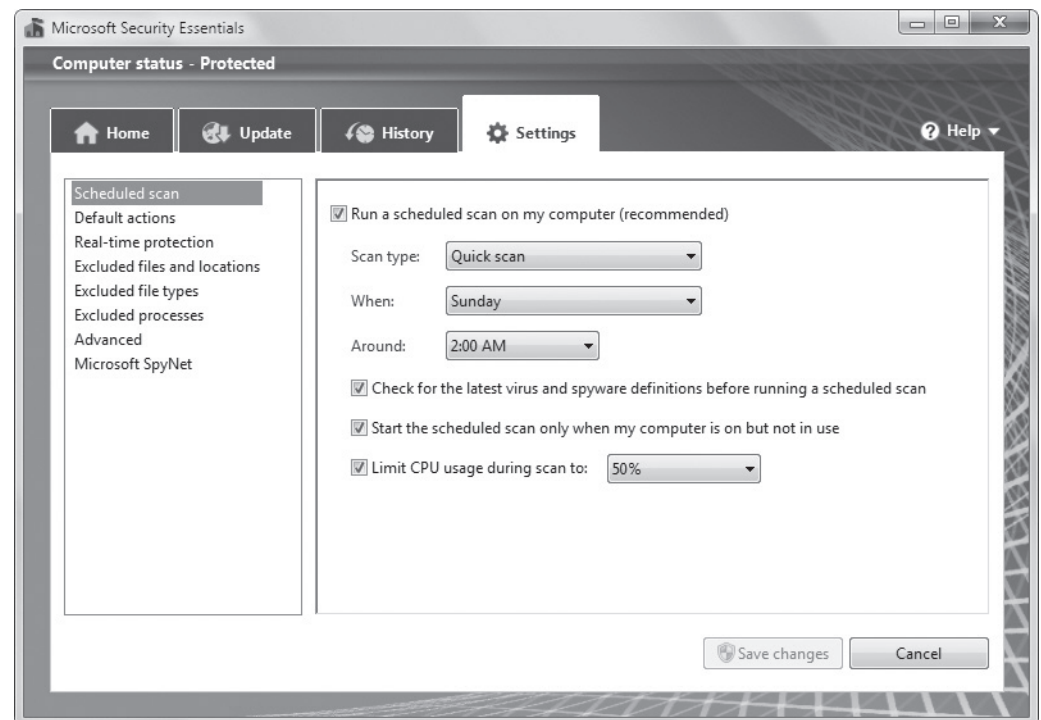
CONFIGURE MICROSOFT SECURITY ESSENTIALS

GET READY. To configure Microsoft Security Essentials, perform the following steps:

1. In Microsoft Security Essentials, click the **Settings** tab.
2. To change the schedule for quick scans, click the drop-down lists to select options (see Figure 7-40). Change the Scan type to **Full scan** and then set the **When** option and the **Around** option, too. It's best to schedule a full scan, which can take hours, to run overnight or on a weekend—whenever you're least likely to use the computer.

Figure 7-40

The Settings tab in Microsoft Security Essentials



3. Change any other settings as you wish. The settings are very similar to those in Windows Defender, which was covered previously.

When you're finished configuring Security Essentials, click the *Save changes* button.

+ MORE INFORMATION

To download Microsoft Security Essentials, go to http://www.microsoft.com/en-us/security_essentials/default.aspx or visit the Microsoft Download Center at <http://www.microsoft.com/download/en/default.aspx>. For details about how Microsoft Security Essentials works, go to http://www.microsoft.com/en-us/security_essentials/ProductInformation.aspx

Using the Malicious Software Removal Tool

If your anti-malware software cannot remove a virus or worm from a computer, try the Microsoft Malicious Software Removal Tool.

CERTIFICATION READY

How is the Microsoft Windows Malicious Software Removal Tool used to remove malware from a computer?

3.3

Computers can become infected even with the best protection software running in the background. If you know your computer is infected with malware, such as Blaster, Mydoom, EyeStyle, or Poison, download and run the *Microsoft Windows Malicious Software Removal Tool*. This utility scans your computer for dangerous malware and attempts to remove it immediately.

You can download the Malicious Software Removal Tool from the Microsoft Safety & Security Center or the Microsoft Download Center. The tools work with computers running Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows Server 2003. If you're running an x64 version of Windows 7, go to <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=9905>.

Download the software to your Downloads folder (or another folder that's easy to access). In Windows Explorer, navigate to the installation file (which may be windows-kb890830-v4.1.exe or windows-kb890830-x64-v4.1.exe) and double-click it. Follow the prompts to install and launch the software.

When the Microsoft Windows Malicious Software Removal Tool window displays, click Next. You have the option of performing a quick, full, or customized scan (see Figure 7-41). Select one and then click Next.

Figure 7-41

Malicious Software Removal Tool scanning options



When the detection and removal process is complete, the tool displays a report that indicates which, if any, malware was detected and whether it was removed. Click Finish.

Microsoft releases an updated version of the Malicious Software Removal Tool on Patch Tuesday each month, or more often if security threats are detected before the next Patch Tuesday updates. Microsoft recommends that you run the tool regularly, such as every week or two, as a supplement to your real-time antivirus software.

A complementary (and free) product is the Microsoft Safety Scanner. This utility also scans your hard disk on demand for viruses and other malware, but is not meant to be a replacement for a full-featured antivirus program such as Microsoft Security Essentials.

+ MORE INFORMATION

To learn more about the Malicious Software Removal Tool and Microsoft Security Scanner, visit <http://www.microsoft.com/security/pc-security/malware-removal.aspx>

Understanding Windows Forefront Endpoint Protection

Microsoft Forefront Endpoint Protection works with System Center Configuration Manager 2007 to provide security for network-connected computers in the enterprise.

CERTIFICATION READY

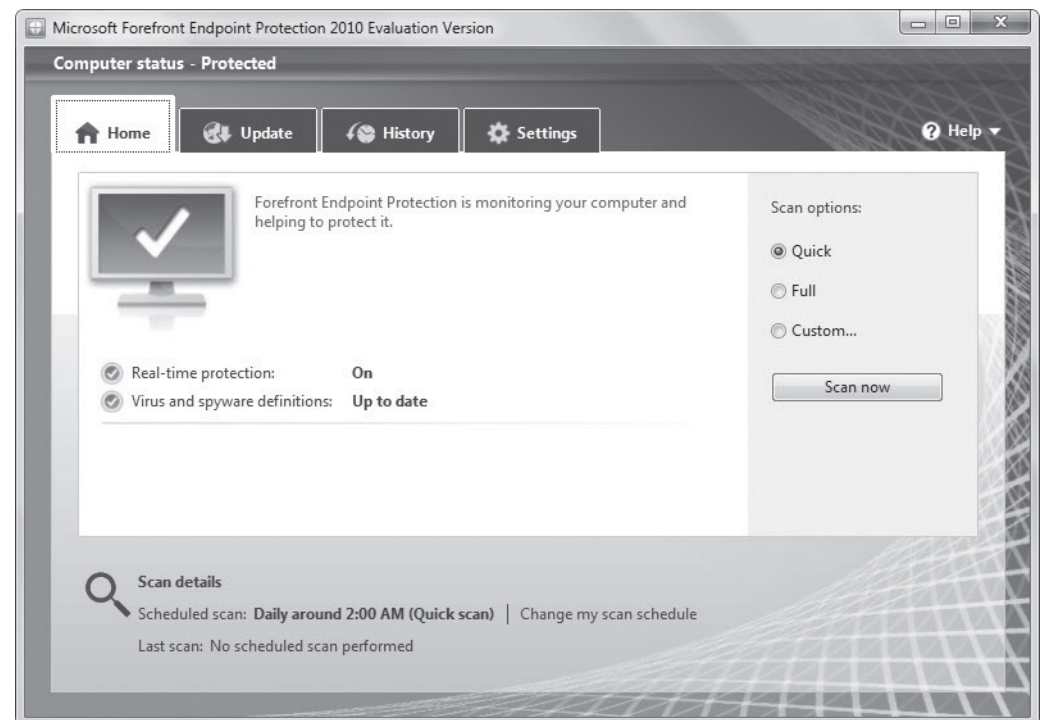
How is Microsoft Forefront Endpoint Protection used to protect client computers in the enterprise?

3.3

Microsoft Forefront Endpoint Protection is a combination of antivirus/anti-malware and management software for desktops, laptops, and other client *endpoints* in a business environment. If you have more than 10 client computers to protect in your organization, Microsoft recommends that you use Forefront Endpoint Protection rather than Microsoft Security Essentials. The client interface for Forefront Endpoint Protection 2010 is shown in Figure 7-42.

Figure 7-42

The Forefront Endpoint Protection 2010 client interface



Forefront Endpoint Protection 2010 is built on System Center Configuration Manager. Configuration Manager provides centralized management of client computers along with the ability to secure them, and it supports WSUS for distributing Windows updates and hotfixes. In busy organizations with 10, 20, 30, or more client computers to manage, administrators have a hard time staying on top of management and threat-detection tasks if they must visit each computer physically. Forefront Endpoint Protection allows most management and security updates and tasks to be performed over the network, using automated tasks and policies that apply to many computers at once.

System Requirements

Forefront Endpoint Protection 2010 requires a Microsoft System Center Configuration Manager 2007 site that has Forefront Endpoint Protection Server installed. The following systems are fully supported:

- Windows 7 (x86 or x64)
- Windows 7 XP mode
- Windows Vista (x86 or x64) or later versions
- Windows XP Service Pack 2 (x86 or x64) or later versions
- Windows Server 2008 R2 (x64) or later versions
- Windows Server 2008 R2 Server Core (x64)
- Windows Server 2008 (x86 or x64) or later versions
- Windows Server 2003 Service Pack 2 (x86 or x64) or later versions
- Windows Server 2003 R2 (x86 or x64) or later versions

You can also install Forefront Endpoint Protection 2010 on the following operating systems, with some limitations. You have to install the software manually, you cannot manage the clients centrally, and you cannot apply policies to them:

- Windows 7 Starter
- Windows 7 Home Premium
- Windows Vista Basic
- Windows Vista Home Premium
- Windows XP Home Edition

Deploying to Clients

You can install Forefront Endpoint Protection directly (manually) on client computers that are not running the Configuration Manager agent, or you can run the installation software from a server in a domain environment with Forefront Endpoint Protection Server installed. Remember, if you install the software directly on client computers, you will not be able to manage the clients centrally nor apply policies to them.

To deploy Forefront Endpoint Protection to client computers in a domain, you must verify prerequisites, uninstall any existing antivirus software, create Forefront Endpoint Protection policies, configure Forefront Endpoint Protection definition updates, deploy the Forefront Endpoint Protection client software, and verify that the deployment was successful.

Microsoft recommends the following general steps for deploying Forefront Endpoint Protection to clients in a domain environment:

1. Create Forefront Endpoint Protection policies according to your organization's requirements, set policy precedence, and then assign policies to one or more deployment collections.

2. Configure Forefront Endpoint Protection definition update methods based on the settings defined in the Forefront Endpoint Protection policies created in Step 1.
3. Deploy the Forefront Endpoint Protection installation package to client computers.

With Forefront Endpoint Protection deployed, you can perform a quick or full scan on one or more computers simultaneously from the Configuration Manager console.

+ MORE INFORMATION

For more information about Microsoft Forefront Endpoint Protection, visit <http://www.microsoft.com/en-us/server-cloud/forefront/endpoint-protection.aspx>

SKILL SUMMARY

IN THIS LESSON YOU LEARNED:

- Windows 7 comes with many built-in maintenance tools that help to keep computers running at top performance. These tools include Disk Defragmenter, Disk Cleanup, Task Scheduler, and the Action Center Maintenance feature.
- Disk Defragmenter can speed up your computer's performance by defragmenting data on your hard disk. In Windows 7, the utility is set to automatically run once a week.
- Disk Cleanup helps you remove unnecessary files from your computer, such as downloaded program files, temporary Internet files, those that are left after running software, and much more.
- Task Scheduler enables you to automate tasks that don't have scheduling features built in. You can also use Task Scheduler to open programs on specific days and times, or at Windows startup.
- Windows 7 Action Center is an improvement upon Security Center in previous versions of Windows. Within Action Center, you can view the status of security features (firewall, antivirus software, etc.) and maintenance (backups, updates, etc.).
- System Information displays a wealth of information about your computer's hardware, drivers, and system software. If you're having any type of system-related issues, you should check System Information for possible clues as to the source of the problem.
- The Windows registry is a database of configuration settings for your computer. The registry is self-sufficient and rarely requires maintenance, but you can use a reputable registry cleaner occasionally to remove settings that are no longer used.
- Microsoft provides several ways to help you keep your Windows system patched and updated, using hotfixes, service packs, updated drivers, and more. Windows Update and Microsoft Update are the primary update tools.
- Windows Firewall is the native firewall in Windows 7 and many other versions of Windows. It monitors inbound and outbound traffic to allow safe traffic to flow and to prevent unsafe traffic from reaching your computer.
- Windows Defender is a free program from Microsoft that monitors your computer for spyware and quarantines or removes it upon detection.
- Microsoft Security Essentials is another free program from Microsoft that provides constant, real-time protection from viruses and other malware.
- If your anti-malware software cannot remove a virus or worm from a computer, try the Microsoft Windows Malicious Software Removal Tool.
- Microsoft Forefront Endpoint Protection works with System Center Configuration Manager 2007 to provide security for network-connected computers in the enterprise.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. A disk that is _____ has file data spread across many different sectors.
2. _____ is a utility that removes many different kinds of unnecessary files from your computer.
3. In Task Scheduler, a _____ is an event that causes a task to run.
4. The _____ is a database in Windows that stores user preferences, file locations, program configuration settings, startup information, hardware settings, and more.
5. Microsoft provides regularly scheduled updates to the Windows operating system via the _____ feature.
6. _____ delivers updates for Microsoft software in addition to the Windows operating system.
7. _____ describes a wide variety of malicious software, such as viruses and worms, that attack computers.
8. A _____ is a collection of updates from Microsoft since the last version of Windows or another Microsoft product was released.
9. _____ is Microsoft's free antispyware program.
10. _____ enables you to centrally manage the security of client computers and devices in an enterprise.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which Windows built-in utility helps you delete unnecessary files from your computer?
 - a. Disk Defragmenter
 - b. Disk Cleanup
 - c. Task Scheduler
 - d. Registry Editor
2. Which Windows built-in utility helps improve your computer's performance by moving sectors of data on the hard disk?
 - a. Disk Defragmenter
 - b. Disk Cleanup
 - c. Task Scheduler
 - d. Registry Editor
3. In Task Scheduler, which command creates a task using a wizard?
 - a. Create Task
 - b. Create Scheduled Task
 - c. Create Task Automatically
 - d. Create Basic Task
4. In Windows Defender and Microsoft Security Essentials, which of the following scans is *not* available?
 - a. Quick
 - b. Full

- c. Partial
 - d. Custom
5. Which of the following is *not* part of the Maintenance section in Action Center?
 - a. Check for solutions to problem reports
 - b. Virus protection
 - c. Backup
 - d. Check for updates
 6. If Action Center detects a maintenance or security issue that needs your attention, an X is displayed under the flag in the notification area. What color is the flag?
 - a. Red
 - b. White
 - c. Yellow
 - d. Orange
 7. How often does Disk Defragmenter run by default?
 - a. Every day
 - b. Once a week
 - c. Biweekly
 - d. Once a month
 8. Which program is always updated on Patch Tuesday?
 - a. Windows Defender
 - b. Microsoft Security Essentials
 - c. Malicious Software Removal Tool
 - d. Windows Firewall
 9. If, for example, your computer is infected with MyDoom, which tool should be used to remove it?
 - a. Malicious Software Removal Tool
 - b. Windows Firewall
 - c. Windows Defender
 - d. Task Scheduler
 10. Which system does Microsoft Forefront Endpoint Protection require?
 - a. Windows Server 2008 R2
 - b. Windows Server 2008 R2 or later versions
 - c. System Center Configuration Manager 2007
 - d. Windows 7

True / False

Circle T if the statement is true or F if the statement is false.

- | | | |
|---|---|--|
| T | F | 1. Microsoft includes Windows built-in maintenance tools in the Maintenance Tools folder in Accessories. |
| T | F | 2. Disk Cleanup can be run on demand but the utility does not have its own scheduling feature. |
| T | F | 3. Windows Update provides hotfixes and service packs for Windows computers. |
| T | F | 4. Windows Defender can run simultaneously with Microsoft Security Essentials, as a complementary program. |
| T | F | 5. Windows Firewall is enabled automatically in new installations of Windows 7. |

■ Competency Assessment

Scenario 7-1: Automating Computer Maintenance and Program Launching

Maria is a busy freelance writer who uses her computer many hours a day to research and write articles for several national magazines and newspapers. Her computer, which runs Windows 7 Professional, must be running at peak performance with little downtime. Maria has little time to devote to computer maintenance tasks. She also uses Internet Explorer 9 and Microsoft Word 2010 every day and would like them to start automatically when Windows starts. Maria asks you for advice how to maintain her computer with relatively little effort, and how to configure her computer to start programs automatically. What do you tell her?

Scenario 7-2: Removing Viruses Safely

You are a support person for a computer consulting company. Rajeem is an independent tax consultant who calls you to report that he believes he infected his computer with a virus after downloading and installing a tax-related utility from the Web. How do you advise him to check his computer and resolve the problem, if necessary?

■ Proficiency Assessment

Scenario 7-3: Gathering System Information

In an effort to troubleshoot an issue on a client computer, you posted a message on an online PC support forum. The forum moderator posts a message asking you to list all of the programs that launch at startup on the affected computer. What is the easiest way to provide this information?

Scenario 7-4: Distributing Windows Updates Across a Network

You support Richman Investments, a brokerage firm that employs 20 brokers. Each broker has his own client computer, and the firm has a server running Windows Server. All of the client computers are configured identically.

Over the past six months, some Windows updates have caused the computers to hang, leaving the brokers without computers to conduct business. How can you ensure that the Windows updates that install on client computers will not cause usability issues?